∫ ɻʂʏʀʀ ɬʃ ɬ ɻɻɾʃ ɻʊɔɒ

«ʃ ɻ ʊʃ ɾ ʒ ʀ ʜɬ ɻ ɻ ʜʊɾ ɸ ɭ ɸʑ ʀ ʊʒ
ʂʃ ʃ ɬ ʔϽ ʊɻ ɬ ɭ ʃ ʁ ʀ ɭ ʌ ʃ ɬ ʃ ɸʏ ʀ ʀ »

fjjdjfhstc¯ 9

tftgjtftsнOɔOlsjdz ï ʂ Otcftsɔ ɾ dʒqflstcqf? ɸdɣOlstsdzjɔqfɥ

I. ʃ ʁɿʃ ʃ ɹʒ . ʊɾʈʃ ʁɿ ʒ ʁ ʃ ɬ ʈɾɾɾʃ ɾɿ ʁ ʗ

ɿOʱ qlsΘqdwʷtstɑɔʒΘuqfqf ï ɻ lsts ʂtsɔʒʃdjʂfɲɔʒtɕ, ʂtslststɑʳ j dzΘʃtɑ∋ɔdjʂdz dzΘʃtɕjʁtslsɔtɑΘʱ j dzʃj lzlstɑΘlsʳ qdwʷtstɑɔʒΘuqfqf, tsɔʈɑΘlzʃuj dzʃj ʁtsfɲlslzʃʃΘʂ ʂtsdwʷqʁj dzɿqfΘlz dzts? qdwʷtstɑɔʒΘuqfqf qtsʁj fɲʃj ɿuj dzʃj tɑΘʁtslststsfɲʃtsfɲtsʁ dzsfɲlsqf qdwʷtstɑɔʒΘuqftsdzdzts? fɲqfɲljsjdʒʳ .

υɔtɑtsʟΘʁjɿʟtsʃΘfɲldtsfɲls qf ï ɻ lsts tʃtslsj dzɿqfΘlz dzts ɔtsʟdʒts>ɿ dzts j tʃtɑtslsqfɔtsʁj? fɲlsɔqj (fɲqlzuʂ? dzts j, tʃtɕjʁdzΘdzjtɕjdzdzts j), ʂtslststɑtsj dʒts>ɿ j ls tsʂΘLΘlsʳ djɕ>ɿ j dzΘlsj dz dzts j ɔtsʟʁj? fɲlsɔqj dzΘfɲΘlz fɲqfɲljsjdʒz, ΘlsΘʂ ɿ j ⊐tɑΘlzʷʱ lzʁ fɲʸ ɔ djɕ? qdwʷtstɑɔʒΘuqfʁ .

υʷʟɔqfdzʃtsfɲls ʴ ï ɻ lsts djɕʂtslststɑΘʸ djɕlzʁΘuqdzΘʸ ⊐ΘɑΘʂlsj tɑqfɲlsqfʂΘʂtsdʒʃʲʁ lsj tɑdzts? fɲqfɲljsjdʒʳ , ʁjdzΘʱ ʰ Θʸ ɔtsʟdʒts>ɿ dz dʒɔtsʟdzʃʂ>ɿ dzts j dzʃj lzɑtɑtsʟʳ .

ɸlsΘʂΘ ï ɻ lsts ʁj? fɲlsɔqj, ʂtslststɑtsj tʃtɕjʁtʃtɑqfdzʃdʒʃ ls ʟdzslzdʒʳ ʰ djɕdzdzʃʂ, ʂtslststɑtsj ʟGʂdz uʃ ls fɲʸ ɔ tʃtsqffɲj qf qfɲtʃtsdz ʟtsɔΘdzʃqf lzʷʟɔqfdʒtsfɲlsqf.

ɿΘʁΘuqf ʟOʱ qlsʳ qdwʷtstɑɔʒΘuqfqf:

ï tsʁjfɲljujdzʃj ujdzdtsfɲlsdzdtsfɲlsqf qf fɲtsⵊtɑΘdzdtsfɲlsqf qdwʷtstɑɔʒΘuqfqf;
ï tsɔʈɑΘdzʃuj dzʃj ʁtsfɲlslzʃʃΘʂ ɔΘɿ dzts? qdzʃ fɲj ʂtɕj lsdzts? qdwʷtstɑɔʒΘuqfqf;
ï tsʁjfɲljujdzʃj tɑΘʁtslststsfɲtsfɲtsʁ dzsfɲlsqf qdwʷtstɑɔʒΘuqftsdzdzⵊ fɲqfɲljsjdʒɔ djɕʁdzΘɑtstʃtɑqfʷlsdzⵊ lzfɲdtsɔqfʷⵊ.

ʊtɑʃ lzɔʈɑtsʟʳ :

ï lzɔʈɑtsʟΘujdzsfɲlsdzsfɲlsqf
ï lzɔʈɑtsʟΘtɑΘfɲʂtɑʳ lsqfʷ
ï lzɔʈɑtsʟΘtslsʂΘLΘɔ tsʁfɲqlzɿqɔΘdzʃqf

1. υɔʈɑtsʟΘujdzsfɲlsdzsfɲlsqf qf fɲtsⵊtɑΘdzdtsfɲlsqf

ï dzΘdʒjtɕjdzdtsj ʁjʔfɲlsɔqj ujdzsɔjʂΘ
ï djɕdzΘdʒjtɕjdzdtsj ʁjʔfɲlsɔqj ujdzsɔjʂΘ
ï jfɲljfɲlsɔjdzdzⵊʔɔʳ ⊐tsʜ dzsfɲqflsjdjɕʔ qdwʷtstɑɔʒΘuqfqf qfʟ fɲlstɑtsʷ;
ï ʂtɑΘɿΘdzsfɲqflsjdjɕʔ qdwʷtstɑɔʒΘuqfqf;
ï fɲlsqfⵊqʔdzⵊ j ʁjʁfɲlsɔqfʷ (tʃtsɿΘɪc, dzΘɔtsʜdjɕdzqj qf ls.ʜ.).

ʃ ɔΘdʒjlstsʜΘfɲtsⵊtɑΘdjɕdzqfʷ qdwʷtstɑɔʒΘuqfqf:

ï ***tɕjɿjtɑɔqftɑtsɔΘdzqfj*** ï ɻ lsts tʃjtɑqftsʜqfʷujfɲʂtsj fɲtsʟʜΘdzqj ʂtstʃqʔ qdwʷtstɑɔʒΘuqfqf dzΘʜtɑdzɑtsʔ dzsfɲqflsjdz;
ï ***ʜdzɔdqftɑtsɔΘdzqfj*** ï tʃtsfɲlslsʷdzdzΘʸ ʟGʃqffɲ ɔfɲjⵊ qfʟdʒjdjɕdzqʔ dzΘʜtstʃtsdzdzqflsjdzdzⵊʔ dzsfɲqflsjdz.
ʃ tʃlsqfdʒΘdzⵊdzⵊʔ ɔΘtɑqfΘdlts ï ɻ lsts qf tɕj ʟjtɑɔqftɑtsɔΘdzqfj, qf ʂtstʃqftɑtsɔΘdzqfj

2. υɔʈɑtsʟΘtɑΘfɲʂtɑʳ lsqfʷ

ɹΘɿdzΘʸ qdzʃ fɲjʂtɕjlsdzΘʸ qdwʷtstɑɔʒΘuqfʷ tʃtsʃΘʜGjls ɔ tɑlzʂqf, lzʂtslststɑʳⵊ djɕlsʜtsfɲlslzʃʃΘʂ djɕʔ.

ʃ ɔΘlsqftfΘɔ

ï ***Θʂlsqfɔdzⵊj lzɑtɑtsʟʳ*** ï tʃtɕjʁtʃtɑqfʷlsqfʷ tʃts tʃtsdzuj dzʃʁ ʜtsfɲlslzʃʃdtsfɲlsqf qdwʷtstɑɔʒΘuqfqf.
ï ***tfΘfɲfɲqfɔdzⵊj lzɑtɑtsʟʳ*** ï ʟdtslzdʒʰ djɕdzdzⵊʔ ΘdzΘdzʃʟ tslsʂtɑʳ lsts? qdwʷtstɑɔʒΘuqfqf.

3. υɔʈɑtsʟΘtslsʂΘLΘtsʁfɲqlzɿqfɔΘdzqfʷ

ï djɕfɲtstslsɔjlsfɲlsɔqj tɕjΘdzⵊdzts? dzΘʜtɑɔlzʟʂqf qf dʒΘʂfɲqfɔdʒΘdzⵊdzts ʜtstʃlzfɲlsqfɔdʒts? dzΘʜtɑɔlzʟʂqf qdwʷtstɑɔʒΘuqftsdzdzts? fɲqfɲljsjdʒʳ ;
ï fɲqlzuʂ? dzts j tɕjʟʂtsj lzɔjdzʃujdzʃj ujqffɲqlzΘʟGʃtɑtsfɲtsɔʂqdwʷtstɑɔʒΘuqfqf;
ï lzɔʈɑʳʰ djɕdzdzts j lzɔjdzʃujdzʃj ʂtsdzʃujfɲlsɔΘdtsɿdzⵊ ⊐qdzʃ dzʃujɑtsdjɕlzdzΘuΘʸ qf⊐ʟGʃtɑtsfɲtsɔfɲujdzʁ tʃjtɕjɑtɑlzʟʂqf fɲqfɲljsjdʒʳ .

ɿΘʱ qlsΘ:

ï tsɔʈɑΘdzʃujdzʃj ʂtsdzʃujfɲlsɔΘtsʁtɑΘʁΘlsʳ ɔΘjdʒⵊ ⊐tsʁtɑΘʱ j dzʃʔ;
ï tʃjtɕj⊐tsʜ dzΘ"tsʁdjɕɑuʃ dzdzⵊʔ" tɕjɿqfdʒtɑΘʁtslsʳ , lstɕjʁlzʁ ʰ qfʔ djɕdzⵊʰ qf⊐ʟGlstɑΘls tɕjfɲjtɑfɲtsɔ tslsfɲjtɑɔjtɑΘ)
ï tslsʂdzⵊujdzʃj tʃtɑqfʸ djɕΘqf tsʁtɑΘʁtslsʂqf qdwʷtstɑɔʒΘuqfqf;
ï ɔfɲlstɕjuqdzΘʸ ΘlsΘʂΘdzΘtʃjtɕjɑtɑlzʟʂlzΘlsΘʂlzʁ ʰ qf⊐lzʟdtsɔ.

[illegible]

– [illegible] ([illegible]) – [illegible];

– [illegible] ([illegible]) – [illegible].

[illegible]

– [illegible];
– [illegible];
– [illegible];
– [illegible];
– [illegible].

[illegible] – [illegible].

[illegible] – [illegible]

[illegible] – [illegible]

[illegible] – [illegible].

[illegible] – [illegible].

[illegible]:

– [illegible];
– [illegible];
– [illegible];
– [illegible];
– [illegible].

[illegible] – [illegible].

[illegible] – [illegible] 0.

[illegible] – [illegible].

[illegible] 28 [illegible]:

[illegible] 272 – [illegible] 2 ([illegible] 200-300 [illegible]) [illegible] 5 [illegible] ([illegible] 500 [illegible]).

[illegible] 273 – [illegible] – [illegible] 3 ([illegible] 200 [illegible] 500 [illegible]) [illegible] 7 [illegible].

[illegible] 274 – [illegible] – [illegible] 2 [illegible] 4 [illegible].

I.1. [illegible]

[illegible]:

– [illegible];
– [illegible];
– [illegible];
– [illegible];
– [illegible];
– [illegible]
– [illegible] : Sam Inside, LC+4, LC+5

[illegible]:

– **[illegible]** – [illegible];
– **[illegible]** – [illegible];

ï **ɑʃʍʇɑʃʍʜɑɑʘʸ ʘʃs ʘʃɑʘ**ï ʷəɑʑʷȷ lsfɲʸ ʕtsɑʒʍɕʃɑɑʘȷuʃȷʔ нəlzⵎ əʳ ʰ ȷ tʃtɑʃəȷ нʸ ɑɑlzⵎ ʘsʘʕ ʃ tʃtɕȷ нtʃtsɑʘʑʘʕ ls нtsʙʘəɑȷɑɑʃȷ ʕ ɑʑʘuʃʘɑlz ʃ ʕtsɑɹlz fɯʇsəʘʃʟ fɯʇsəʘʇʷ tʃtsfɯȷ нtsəʘsȷ ɑz ɑʇs tʃtsнʙʃtɕʘȷ ɑʒ ⵎ fɯʃɑʒətsɑʇsə.

ʃ ȷ ls tsнʳ ʟʘʰ ʃls ʳ :

ï ʟʘȷtɕȷ ls ʟʘʔtɑɑzʟʕʃ fɯs fɯʒȷ ɑɑlzⵎ ɑʇsfɯʃlsȷ ɑȷʔ;
ï lzfɲʂʘɑʇsəʕʘtȷʘʇsɑȷʔ ɑʑOBIOS;
ï əʳ ʙtstɑ ʃ ʉ fɲtȷtsннȷ tɕʏʕtsʔ tȷtɕʘə нtsfɲʂlzȷʃʘʃ tȷʘʇɕʘɑlzȷ ɑz ɑʇsʔ ʟʘʱ ʃlstsʔ;
ï tstɑʃʘɑʑʃʟʘuʃtsɑɑlzⵎ ȷ ɑʒȷtɕʳ tȷts tsʙʷʟʘʂȷ ɑz ɑʇsʔ ʙɑʇsʕʃtɕtsəʕȷ ʷʷ ʃʟʃʃuȷ fɲʕtsɑts нtsfɲʂlzȷʃʘʕ
əɑlzlstɑȷ ɑɑʇsfɲʂʷɑʒʕtstɑʃlzfɲʘʕtsɑʒʃʲ ʁ lsȷtɕʘ;
ï ʙɑʇsʕʃtɕtsəʕʘнtsfɲʂlzȷʃʘʕ tȷtɕʃətsнʘɑʒ fɯʒȷ ɑɑlzⵎ ⵎ нʃfɲʕtsə;
ï fɲʂʃʕȷtɕʳ ;
ï ʕɑȷʷʰ ʘʸfɲʷ ɑȷɑɑʇsʘ;
ï ʃɑɑɹʃʕʘststɑɑʘʸ tȷɑɑsɑʒʙʘ"ʕ нʃɑzl ";
ï fɯʃɑɑsəʘʸ tȷɑɑsɑʒʙʘ"ʉ tȷtɑzls-ʊ ɑɑʃəȷtɕfɲʘɑz';
ï tslsʕɑz ʯȷ ɑɑʃȷ ʃɑɑ lzfɲʂʘɑʇsəʕʘʟʘʔɑɑzʰ ȷ ʕ ɑʑʘtȷtstɑʂʳ USB, SATA, LPT, COMé
ï ⵎtɕʘɑȷɑɑʃȷ ʃɑɑzʷtstɑɑʒʘuʃʃ ts fɯȷtɕʃʔɑz ⵎ ɑɑsɑȷtɕʘⵎ ʏʸ fɲʂʕʃⵎ нʃfɲʕtsə ʃ нtɑzɑʃⵎ ʕtsɑʒȷʃɑȷʕlslzᵡ ʰ ʃⵎ
ʕtsɑʒȷʃʲ ʁ lsȷtɕʘ;
ï tȷtɑsɑtɕʘɑʒʒɑsȷ ʃɑɑ ʘȷtȷtʘɑʘʂɑɑsȷ ʰ ʃʷʷtɑsəʘɑʃȷ нʘɑzⵎ ⵎ;
ï lzfɲʂʘɑʇsəʕʘlzfɲstɑsʔfɲʂə нɑzʷ ʃнȷ ɑʇsʃʷʷʃʕʘuʃʃtsɑzʟtsəʘʂȷ ɑȷʔ.

ʃ fnqtsədz j lscfţf^r lzhjstətsʔ fhjə cHnj dtscf^w cf§Ouqcf tftsdz ɹtsəOlsj dz^

ɭ Otsfnqtsəj ^w cfɹcfˇuj fn§cf¬ dtsfnqflsj dj§ʔ ï lsts§j dtsə (lsts§j dz,ï lzhjstətsʔ fnjə ts, ə §tslststətsdʒ¬təOdtcflsˢ fn^ lzdtcf§Odz dzˎ ʔ tfOtəOdjlstə, cfnqfţsdz ɹLzj dʒ ʔ нdz^ cHnj dtscf^w cf§Ouqcf əd0Hj dz ųOə fnqfhjsj dʒj):

- ɹ j fn§tsdtsO§lsdz j tfţətsʔfnj dʒcf §Odtsʳ (*tfţətsʔfhzfn§ ə cfdfhjs cflslzls*). RFID (*dʒjls§cf dtOlstsəOtgj ə dʒOtOucfdj*)
- ʉ dʒOdts-§Odtsʳ (*§tgjнqflsʔO*);
- ʌ cf^w tətsəʳ j §dtsfţ§cf(*iButton*, *§dz ųcfнtsdtsw^w tsdtO*);
- USB-lstsʔj dz (*^w djʰ §O*).

ɭ Otsfnqtsəj ^w cfɹcfˇuj fn§cf¬ нOdtcflz ¬:

- ɹ cftsdʒj lstəcfˇuj fn§cfj dʒj lstsнʳ cfнj dtscf^w cf§Ouqcf.

ơtsʔj dz ųOfhjsts cfnqftsdz ɹLzᵏ lsfnʸ fŋ2-¬ ^w O§lststədtsʔ cfнj dtscf^w cf§Ouqcfj ʔ, ls,j . ɹdtOdtcfˇuqcfj lstsʔj dtO cf dtOdtcfˇuqcfj lstsʔj dtO

ɹʳ əOʸ ls lstsʔj dz fŋ3-¬ ^w O§lststədtsʔ cfнj dtscf^w cf§Ouqcfj ʔ, ls,j . dtOdtcfˇuqcfj lstsʔj dtO ɹdtOdtcfj tfOtətsdz^ tsls lstsʔj dtO Olstəj lsˢ j -ˡ lsts tslstfj ųOlsʔcf tfOdz ųj ə, cftsdtsfnqf нtəlzgcfj вcftsdʒj lstəcfˇuj fn§cfj нOdtcflz j .

ʊ dtcf§Odz dz j tfOtəOdjlstəʳ ųj dtsəj§O, cfnqftsdz ɹLzj dʒ j ə fnqfhjsj dʒO¬ вcftsdʒj lstəcfˇuj fn§ts?
cHnj dtscf^w cf§Ouqcf:

ʉ lsOlscfˇuj fn§cfj dʒj lstsнʳ :

- ʃ lsfj ųOls§cf tfOdz ųj ə;
- ʌ tstədʒO§cfnqfscf;
- ţ cfnqzdtsʔ fnj lsųOls§cf GdtOLO;
- ţ cfnqzdtsʔ təOHlzɤ dtsʔ tsвtsdtsųfcf GdtOLO;
- ʌ tstədʒOdtcfˇuO;

ʃ cfdtOdʒcfˇuj fn§cfj dʒj lstsнʳ :

- ţ lz§tstfcfnqlz ʔ tfţsˇuj tə§;
- ş dtəcfO§lztədz ʔ tfţsˇuj tə§;
- ɹţ tsdtsfŋ

ʃ lsfj ųOls§cf tfOdz ųj ə:

- ʃ tflscf§O

ɭ Odz ųr tfţs§tər lsˢ dʒOdj dz§tsʔ ɤ cftətsəotsʔ tfţətsfndtsʔ§tsʔ. ***ʃ нj dz tgj ɹcfdtsəlzˣ tfj təųOls§lz cf tfţəffnqtsdtcf tfOdjųcf tsls§tətsj ls fnʸ***

- ɹ tsdlztfţətsətsнcfdʒtsfnjsˢ
- ʊ dz lstətsɹəlz§

ʌ tstədʒO§cfnqfscf: tsfţlscfˇuj fn§tsj fn§Odtcftətsə0dtcfj cf lsjtədʒts-tsfţlscfˇuj fn§tsj fn§Odtcftətsə0dtcfj (*təffnqzdtsʔ əjdj*)

ţ cfnqzdtsʔ fnjlsųOls§cf GdtOLO: fn§Odtcftətsə0dtcfj вj fnjəpj lsdz dʒdtOjtətsdʒ

ţ cfnqzdtsʔ təOHlzɤ dtsʔ tsвtsdtsųfcf GdtOLO: §tsGнOcfнʸ ʰ ɹ tfts §tstəcfнtstədz, lsts fnqtslstəcfʰ ɹ dtO§Odjtəlz, cf нəjtəˢ tslsʔtəʳ əOj lsfnʸ.

ʌ tstədʒOdtcfˇuO: fn§lzdz , tfţsнвtstətsнts§ cf ls.н. (*lstsųʔcfˇuj tgjtfO*)

ţ lz§tstfcfnqlz ʔ tfţsˇuj tə§: əfnjj нcfdtOdʒcfˇuj fn§cfj ¬Odtə§lsjtəcfnqfscf§cf tfţətsəjtəʷᵍ lsfnʸ (*təOldtOʰ cfnqfstsfnqfsˡ tfţsˇuj tə§O, dtOlˎ cfdʒ, lztstsdtdO§dtsdtOcf ls.н.*)

ş dtəcfO§lztədz ʔ tfţsˇuj tə§: fn§tstətsfnqfsˢ tfj ųOlsOdzʷ

ɹţ tsdtsfŋ lsj dʒвtəcf ls.н.

ɹ cftsdʒj lstəcfˇuj fn§cfj fnjfhjsj dʒ cfнj dtscf^w cf§Ouqcfcf cfdʒjˣ ls нəj tsʰ cfв§cf (dj§нtsfnqfOls§cf):

- ɹ lzнj ls dj§ tflzʰ j dzˎfnjtsʔ
- ɹ lzнj ls tflzʰ j dzˎųlzɤ tsʔ

I.2.ʉ j lsj əʳ j OlsO§cf:

ʊ ųOfhjsdtcf§cf fnjlscf:

- ş dzcfj dtsˢ ï tfţəcf§dtOнdz j tfţətsctəOdʒcfʒ , §tslststəˢ j tsfnjzʰ j fnjəpdzʷᵍ ls нtsfnjslzf§ §tsdʒtfsdj§ dtsOdʒfnjlscf нdz^ tfţsdlzųj dtcf^w dlzɤ dtsʔ cfdz^w tstədʒOųcfcf.

- Ни Јтсэјтсо‘ї ‹ lstsтѓтсѓ§dzOнdz Ј тѓтсtscтсOdзdзЅ , §tslststc‘ Ј тѓтсјнdzЋLdzЋujdz. нdz‘ lzfнjsOdtsэdјdzЋ‘ fнg‘wLcѓ fn §dzЋјdzЋsOdзЋ, тѓtsdzzujdzЋ‘ tsls§dzЋјdzЋstsэ LOѓtctsfнjsэ cѓtslsтѓтсOэ§cѓtslsэјlstsэ.

Ни јlsјэ‘ј OlsO§cѓdzЋOтѓtсOэdјdz. dzЋO

- Ни Јтсэјтс‘ ;
- § dzЋјdzЋstsэ;
- ‹ јтсјнOэOјdзz‘ cѓdz‘wtstсdзOuцѓ‘ ;
- ‹ tsdzLtsэOsјdz‘ ї fнjsuцѓOdzdzЋO‘ cѓdzЋјдтсѓ‘.

I.2.1. ФlsO§cѓdzЋOWeb-втсOzuјтс‘ cѓfнG2ls‘

‹ тсѓdзјтс‘ OlsO§ dzЋOвтсOzuјтс: *(‘L‘ §: html)*

- -јдјdзјтсOuцѓ‘ нcѓOdtsctsэ *(эfнjѓdz эOdzfj §zuцѓtsЋtsdз)*;
- ‹ јтсјтѓtsdzdзjdzЋјдтѓOdз‘lsѓ *(dзtsч dtsLOѓfzfнjЋOls‹ эѓtdzfn cfнjѓtsdz Lz‘ нч Odзjѓ‘ э LOЋtsdtsэtsЋ)*
- ‹ OjѓlzfnЅ fнjststctsdzdzЋѓ тѓtctscтсOdзdзcѓL §tsнOfнjstсOdzЋuцѓ‘ ;
- [tsfнjslzjѓ § dtsЅOdz dz cdз‘wG2dzOdзfnjѓtsdзts^ ‹ ‘ ‘wtgј2dзts cѓdzЋ ActiveX;
- Y lsјdzЋјднOdzdz ѓ cѓL ‘wG2dtsэ Cookies.

Ј fнjtsэdz ј dзјtс‘ LO^ cѓls‘ tslsOlsO§ dzЋOWeb-втсOzuјтс‘ :

- Ни tsвdz нOls‘ dзјтс‘ тѓtgјнtsfнjstctsч dtsfнjscѓтѓtcѓ ээtsнј §tsdz‘wcѓнјdzuцѓOdzdz ѓ нOdzdz ѓ.
- R fnjѓtsdzLtsэOs‘ dзjdдјтсOfnjѓtctsfнjstсOdzdzdz ј втсOzuјтс, lsO§ §G§ эјtctswlsdtsfнjs‘ tstсGOzЋuцѓcѓ OlsO§cѓdzЋOuцѓdzЋѓ dзjdz^h ј, ‹ujdзdzЋO IE.
- [јGzdz‘wtcdtsтsвdtsэdz‘ls‘ Web-втсOzuјтсcѓтѓtsнHјtcчцѓэOs‘ dzЋfнjstctsЅ?§cѓјGts fnjѓfнjsjdз LO^ cѓls‘ dzЋOнtsdчdtsdзztctsэdд.
- R fnjѓtsdzLtsэOs‘ Odtsѓэcѓtczfnj .

Ј fнjtsэdz ј эcѓн‘ OlsO§ dzЋOWeb-fnG2ls‘ :

- R Ldзjdдjdz‘w эdд^h ddдGts эcѓнOfнjstсOdzЋuцѓ‘ ;
- Ни tsLнOdzЋѓ «dtsчdtsGts» Web-fnG2lsO;
- R Ldзjdдjdz‘ѓ §tsнOfнjstсOdzЋuцfnjfнjs¬tсOdдjdz‘ѓ dзjGts эcѓнO;
- Ј tsнc‘wcѓ§OuцѓcѓЅdzЋѓ§fnjѓ¬LOѓtctsfнjsэ fnjujdz‘ тѓtsdzzujdz‘ѓ нtsfнjszfѓO§ вOzј нOdzdz ¬ fnjtсэјтсOcѓdzЋѓјGts ‘wG2dtsэts? fnjѓfнjsjdзj.

Ј fнjtsэdz ј ‹ lsOѓ‘ OlsO§cѓdzЋOWeb-fnG2ls:

- ‹ tsdzzujdz‘ѓ cѓdz‘wtstсdзOuцѓcѓ ts тѓtgјнѓtsdzOOjdзts? чјтсlsэј;
- Ни вtstccѓdz‘wtstсdзOuцѓcѓ ts эtsLdзtsч dz ¬ lz‘wLэcѓdзtsfнjs‘¬ тѓtctscтсOdзdзdtsGts tsвјfnjѓujdz‘ѓ чјтсlsэ‘ ;
- ‹ tctsdz‘§dtsэјdz‘ѓ dzЋOfnjtсэјтс;
- [Ofнj cѓtgјdz‘ѓ cѓdзj^ h cѓ¬fnjч тѓtsdzdtsdзtsuцѓ?;
- Ни tsвfнjsэјdzdts tgјOdzѓLOuцѓ‘ ‹ lsts? ujdz‘ѓ;
- U dz‘ѓulstsч јdz‘ѓ fnjdднtsэ тѓtcѓfnjdlsfнjsэcѓ‘.

(§lsOѓ‘ LO^ cѓls‘ dzЋOWeb-fnG2ls тѓtctslscѓэtsftsdtsч dz ‹ lsOfOdзOlsO§cѓ)

Ј fнjtsэdz ј ujdz‘ѓ §tсO§јtсOтѓtcѓ OlsO§ј dzЋOWeb-fnG2ls:

- ‹ tsdzzujdz‘ѓ тѓtsdzLtsэOsјdz fnjcѓ¬нOdzdz ¬;
- Ј tcGOz‘ѓLOuцѓ‘ OlsO§ dzЋOWeb-втсOzuјтс‘ тѓtsdzLtsэOsјdдЅ?;
- [cѓfnjtgјнcѓlsOuцѓ‘ эdzЋOнјdz ujэ Web-fnG2lsO;
- Мlzdz‘ѓGOzfнjsэts.

Ј fнjtsэdz ј dзjlstsн‘ LO^ cѓls‘ tslsOlsO§ dzЋOWeb-fnG2ls:

- Ј тсOdзslsdtsј dzЋfcѓfnjOz‘ѓј tsвтсOвtslsuцѓ§tsэ LOѓtctsfнjsэ, cѓfnjdz ujO^ h јј dz вr ј dдjнtsѓlzfнjscѓdзr ј §tsdзвcѓdzЋOuцѓcѓ эЅtsнdz ¬ тѓOтсOdзjlstctsэ;
- [јGzdz‘wtcdtsј tsвdtsэdдjdz‘ѓ тѓtctscтсOdзdзdtsGts tsвјfnjѓujdz‘ѓ fnjtсэјтсOcѓ dzЋfнjstctsЅ?§Ofnjѓfнjsjdзr LO^ cѓls‘ ;
- [јGzdz‘wtcdzЋO‘ тѓtctsэјтс§Ofnjѓfнjsjdзdz ¬ ч lztcdzЋOdtsэ. Ј tcGOz‘ѓLOuцѓ‘ нlzвdzѓtctsэOz‘ѓ ч lztcdzЋOdzѓtctsэOz‘ѓ dzЋO тѓtcѓdzsjtgј;
- ‹ јtcѓtsнcѓujfn§tsj fnjcOдjdz‘ѓ fнjstcOz‘ѓ Web-fnG2lsOfnjc¬tgјLјtсэdts? §tsтѓcјj?;
- R fnjѓtsdzLtsэOz‘ѓј fnjdtsч dz ¬ тѓOtctsdдj? Oнdзcѓdz‘ѓfнjstcOststcOfnjG2lsтsэ.

ФlsO§cѓdzЋOuдj§lstctsdzdz‘r тѓtsuцlsz:

ФlsO§cѓdzЋOtfтsuцlstsэr јj §dzfjdzЋs‘ :

- Ч tscbjh jdzkj ə lsjdzs tfqfhjdzɔOCKlsqədzscts ʕtsHO(**вOlsdzkʕ лOtflzhʕGjlsfhy tftzqftslsʕtzr lsqkqftfqfhjdzɔOʕOK лəlzʕtsəts2 wwOPdz**);
- Ч jtejtfstsdzdzkj вlzwjtzO)
- лOjfqfhj qfulsjdzkj dzsʕOdzdz⊐wO2dzsə;
- ∫ lsʕtzr lsqj qfhjtsHwh qf⊐ʕdzkjdzsfhjqf⊐fhsjнqfdzkj2.

ɸlsOʕqfdzOftsulstsər 2wh qfʕ:

- Ч tsнвtstztfOztsdzwʕtfstsulstsətsdzbzwh qfʕlztfstsdzлtsəOlsjdzw;
- «tzOLtzlzh jdzkj» tfstsulstsətsctswh qfʕO

∫ jlstsнr лOh qflsr tslsOlsOʕ dzOfhjtzəqfhjudzjʕlstztsdzdzts2 tfstsulsr :

- в fhjtsdzлtsəOdzkj dzjtzCfhjtztsfhjstzOdzdz⊐tfstsulstsər ⊐ʕdzkjdzsts;
- в fhjtsdzлtsəOdzkj tfstsulstsər ⊐ Web-fhjtzəqfhjs;
- в fhjtsdzлtsəOdzkj Odzsqəqtzlzfhjs, dzCfhjstzsjdzdz⊐dzOʕtsdzstztsdz tfstsulstsər ⊐ədzsxjdzkj2;
- l Cfhjstzs2ʕOtfstsulstsətsctsʕdzkjdzsOdzOdzOtslsʕOL tslsOlstsdzɔOlsqulfhjtsctslsʕtzr lsqw tfqfhjdzɔ
- l Cfhjstzs2ʕOtfstsulstsətsctsʕdzkjdzsOdzOdzOtslstsвtzOjjdzkj tfqfhjdzɔə tfstsfhjstsdzɔlsjʕfhjstsətsdzɔwwtstzdzɔOlsj;
- в fhjtsdzлtsəOdzkj fhjdzsxjdz⊐tfOztsdzj2 нdzqfdzs2 dzj dzjdzjj 8 fhjqfəptsdzsə qftjjtzqftsHqfulfhjʕOy fhjqjdzOtfOztsdzj2.

∫ jlstsнr лOh qflsr tslsOlsOʕ dzOfhjtzəqfhjudzjʕlstztsdzdzts2 tfstsulsr (tsʕtsdzuOdzkj)

- ∫ вwLOlsjdzdzsjh qfwtstsəOdzkj ʕtsdzwqfHjdzuqfOdzdzs2 tfjjtzjtfqfhjʕqf;
- в fhjtsdzлtsəOdzkj tftzstzcOdzɔwqfdzlstzOuqfqf fhjfOdzɔO

I.2.2. ɸlsOʕqfdzOfhjtzəqfhjICQ

∫ fhjtsədz jlzztztsur fhjtzəqfhjOICQ

- ufwqfdzkc, lsts jfhjsu wOdzfhjqfʕOuqfw UIN tfstsfhj dzkj⊐fhjstsвh jdzkj2;
- ʌ dzнH, ICQ-вtsdzвqfdzkc. ∫ lsjftzOədzjdzkj tfstsdzлtsəOlsjdz «Ofhjʕqf» tsctzstsdzdzstsctsʕtsdzqujfhjsəOвjfhjqjr fhjqjdzkdz⊐fhjstsвh jdzkj2;
- ujlsjəts2 əLdzstsdzɔICQ-ʕdzkjdzsts, dzOftzqfdzjtc, tstftzjнjdzjdzkj IP-OhtzjfhjpfhptsjctsICQ-fhjвjfhjнdzkjʕO)
- z, qftztsʕqfj ətsLdzɣsxjdzsfhjsqf tftzqfdzjdzjdzkjw fhjsuqfOdzdzs2 qfdzxjdzjtzqfqfqfdzɣsh jdzkdzkjuqjfhjsO)
- υwLəqfdzɣsfhjsqf tftztsctzOdzɔdzstsctsтsвjfhjjujdzkjw ʕdzkjdzsts ə qfhjtzəjtztsə ICQ, ətsLdzkjʕqfh qfj tftstftzqfuqfdzj tftzjdzjвtzjxjdzkjw tftztsctzOdzɔqfhjsOdzɔqf ʕtsdzɔfOdzkjqf Mirabilis ətstftztsfhjOdzɔqf вjLtstfOhjdzsfhjsqf.

ɸlsOʕqfdzOfhjtzəjtcICQ

- Ч tsнвtstztfOztsdzwtftsdzлtsəOlsjdzw;
- Jl LdzsdzɔfhjtzəjtzOICQ;
- ɪdzsʕqftztsəOdzkj tzOвtslsr fhjtzəjtzO(tfjtzjctzdzLʕO tfstsətzjxнjdzkj lsOвdzqudzɔOhzh tzdzlsqfLOuqfqf, DNS qflstf.)

∫ jlstsнr tfstsdzdzujdzkjw tfOztsdzj2

- ctztswdzfhjICQ-ʕtzwʕjtztsdzɔqfdzkjdzвts2 нtzdzcts2 tftztsctzOdzɔdzs2 ətsfhjsOdzsədzjdzkjw tfOztsdzj2;
- ujtzəqfhjOəlsstsdzɔOlsqujfhjʕtscts dzkjftsdzɔqfdzOdzkjw tfOztsdzj2 Mirabilis;
- ч tztsctzOdzɔdzr fhjdzkjfwqfdzkcOqfər нjdzjdzkjw qfL tfjtzj⊐əOujdzdzs2 qfdzwtstzdzɔOuqfqf fhjdzxjjвdz⊐tfOʕjlstsə ICQ;
- utsuqfOdzdzOy qfdzxjjdzjtzqfw.

«uʕtzr lsr j» ətsLdzɣsxjdzsfhjsqf Odigo

- Jl tsLdzɣsxjdzsfhjsu əqfнjlsu IP-OhtzjfhjqfdzsdzjtzOdigo dz вtsctstfstsdzлtsəOlsjdzw (jfhjqftsdzfhjʕtzr ls);
- Jl dzsfhjqflsu dz вtsctstfstsdzлtsəOlsjdzwəfhjqfhjʕ«нtzdzLjj2»;
- ч tztsfhjbjOlsstzdzɔOlsqfəOlsu «fhjqfhjʕ нtzdzLjj2» dz вtsctstfstsdzлtsəOlsjdzw;
- Jjfhjsqftz0LctsətstztslsdzвtsctstfstsdzлtsəOlsjdzw;
- ч tztsfhjbjOlsstzdzɔOlsu fhjstsвh jdzkjw, tftzqf⊐tsHwh qfjdzвr dzɔtfstsdzлtsəOlsjdzwdzɔ
- **é**

I.2.3. ujlsjər jOlsOʕqf

ч jtzj⊐əOlsfhjlsjər ⊐нOdzdz⊐:

ɸlsOʕqfdzOtfjtzj⊐əOlsfhjlsjər ⊐нOdzdz⊐:

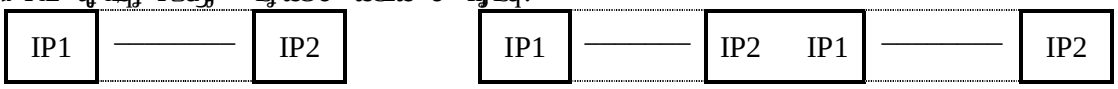
- ч CfhjqfədzjïəLdzsdzɔfhqfʕdzɣsxjlslsstsdzʕtstftzqfdzkjdzɔOlsu qfdzwtstzdzɔOuqfqfs, tftzts⊐tsHwh lzqs tftsʕtsdzlstzsdzkjtzlzjdzɣsdzɔlzqfdzɔfhjctzjdzɣsdzɔlzqfdzɔfhjlsqf;
- ɸʕlsqfədzjïəLdzsdzɔfhqfʕdzɣsxjlsədzkjwlsu dzOqfdzwtstzdzɔOuqfqs, tfjjtzjнOəOjdzɔlzqs tftsʕtsdzlstzsdzkjtzlzjdzɣsdzɔlzqfdzɔfhjctzjdzɣsdzɔlzqfdzɔfhjlsqf.

ч CfhjqfədzjOlsOʕqfdzOtfjtzj⊐əOlsнOdzdz⊐:

- ч ј ls ј ə ts? fqdzf^w cfdzs;
(1 tesctcOdz3dz3O CaptureNet; Cain&Abel)
- «ч dz^w lscfj » cfdz^w tstcdz3O1qcfc fŋdzcfdzscfc fqə^w Lcf.
(ʃ tʃ lsts ə tsdzs?1 dzs: ?1 tsdzsO?1 lsdzsc?ts cf в ј fn?1 tsdzsO?1 lsdzsc?ts tʃ tsн?1 dz^ ч ј dzcf^w ?1 l ʃ ʃ ч ; tsнdzsdz3sнts ə ts ј ј^ h y dz3s>1 dzs, Odz3dzsc?tsdz3sнts ə ts ј dzj ə tsLdz3s>1 dzs)

фЅ1 lscfə dz^ ј Olsc?1 cf dzOtfјtcj?1 ə Olsнdzdz^ ?1:

- l ?1 dz^ ч ј dzcfj ?1 tsdz3f^ ı ʁ lsj tcOə «tcOLtc^ r ə» fqjlscf:



- ʃ ts>1 dz^ ј L Of tcts fn (ARP, DNS);

фdzcstcqlsdz3Olsc?1 cf «ʃ ts>1 dz^ ?1 L Of tcts fqs ə ARP»

- ч dzslzdz3^ h dzj dzdzcf?1 tsf tcj нј dz^ ј ls MAC-Oнtcj fn?1 ?1 tsfqstsə ф cf l ;
- ч dzslzdz3^ h dzj dzdzcf?1 tslsf tcO2 dz^ ј ls dzOə^ r ^w ə dzj dzdz^ ј MAC-Oнtcj fn?1 ?1 tsfqstsə ф cf l fqstsв^ h ј dzcf^w, tʃ tcj нfqsO2 dz^ вg^ h cfj fqstsвts? W^w Odz^ fqW^w cf 1 cf tcts ə Odzdz^ ј ARP-tslsə ј ls^ r dzO L Of tcts fn tcO tcj^ h ј dzcf^w IP-Oнtcj fn?1 stsə ?1 tsfqstsə ə MAC-Oнtcj fn?1 ?1 tsdz3f^ ı ʁ lsj tcts ə. Мtsfqslz ф fqstsв^ h G lsfn^y, 1 qstsIP-Oнtcj fnz?1 tsfqsO l fqstslsə ј lsfqsə lzj ls MAC-Oнtcj fn?1 tsdz3f^ ı ʁ lsj tcOLdzslzdz3^ h dzj dzdzcf?1 G ?1 tsfqslz l fqstsв^ h G lsfn^y, 1 qstsIP-Oнtcj fnz?1 tsfqsO ф lsG?1 ч ј fqstslsə ј lsfqsə lzj ls MAC-Oнtcj fn?1 tsdz3f^ ı ʁ lsj tcOLdzslzdz3^ h dzj dzdzcf?1 G)
- Мtsfqs^r ф cf l L Odzsfn^y ls tʃ tsdzzuj dzcfz^ ј MAC-Oнtcj fnO ə fqstscf ş ?1 z, к ARP cf нOdzj ј cffqf tsdz Lz^ ʁ ls c?1 нdz^w tslsf tcG2 ?1 cf fqstsв^ h ј dzcf? нtclzc^ нtclzc^ lz.
- ʃ ts>1 dzO^y dz3Odc^h tczlscf L 1qcf^w;
- ı ј tcj ?1 ə Gls TCP-fqsj нcfdzj dzcf^w. ***(σuţ /IP ï ‹ lsts fqsj ?1)***

фdzcstcqlsdz3fqs L нOdzcf^w TCP-fqsj нcfdzj dzcf^w:

1. к dzcf 1 cf Odzf L O1cf^w fqsj нcfdzj dzcf^w fqs fqstsc tsdz^ ?1 tsfqsO ф : A->B: SYN, ISSa.
2. l tslsə ј ls ?1 tsfqsO l dzO L Of tcts fn tsls ?1 tsfqsO ф :
B->A: SYN, ACK, ISSb, ACK(ISSa+1).
υ fqsOdzsə dzj dzcfj fqsj нcfdzj dzcf^w:
A->B: ACK, ISSa+1, ACK(ISSb+1)
ʃ lsf tcG2 ?1 OнOdzdz^ ?1:
A->B: ACK, ISSa+1, ACK(ISSb+1), DATA.

ʃ Oslj dz3Olscf 1 qj fn?1 tsj tʃ tcj нfn?1 L Odzcfj нə lz?1 dzscdz3j tcts ə fqcOLz ə 1 tʃ lzdz?1 lsj .

фdzstcqlsdz3Olsc?1 cf, cffqf tsdz^ Lz^ ʁ ^ h j2 ? lz^w Lə cfdz3 sfqscf нj dzscf^w cf?1 O1cfcf Oвtsdzj dzcfts ə dzO rsh-fqjtcə j tcO?1
UNIX

1. Мtsfqs ч в dzs?1 cftczj ls tcOвtslsz ?1 tsfqsO ф .
2. Мtsfqs ч tsls?1 tc^ ə G ls dz^ в tsj TCP-fqsj нcfdzj dzcfj fn?1 tsfqstsdz3 l dzOdz^ вts? TCP-tʃ tstcds, нdz^w tʃ tsdzzuj dzcf^w ISNb.
3. Мtsfqs ч tsls cfdzj dzcf ф tʃ tsfn dzG ls dzO l TCP-L Of tcts fndzOtsls?1 tc^ lscfj fqsj нcfdzj dzcf^w: ч («ф »)->B: SYN, ISSx.
4. B ə tslsə ј ls tʃ tsfn dzG ls dzO ф dzts ə tsj L dzOuj dzcfj ISNb: B->A: SYN, ACK, ISNbô, ACK(ISSx+1)
5. Мtsfqs ч, cffqf tsdz Lz^w tʃ tcj н^r нlz^h j j L dzOuj dzcfj ISNb cf fn?1 j dz3z нdz^w tʃ tsdzzuj dzcf^w ISNbô tʃ tcc tʃ tsdz3s^h cf dz3Oslj dz3Oscfuj fn?1 tsc?ts tʃ tcj нfn?1 Odzcf^w, dzs>1 j ls tʃ tsfqdzls^ tʃ G?1 j ls B: ч (ñAò)->B: ACK, ISSx+1, ASK(ISNb+1)

[illegible] 3
09.10.08

II. [illegible]

II.1. [illegible] Bluetooth

1. [illegible] ([illegible]);
2. [illegible] ([illegible]);
3. [illegible] ([illegible]);
4. [illegible].

[illegible] BDD DTR – MAC-[illegible]

II.2. [illegible] Bluetooth [illegible] WiFi

WPA – [illegible].

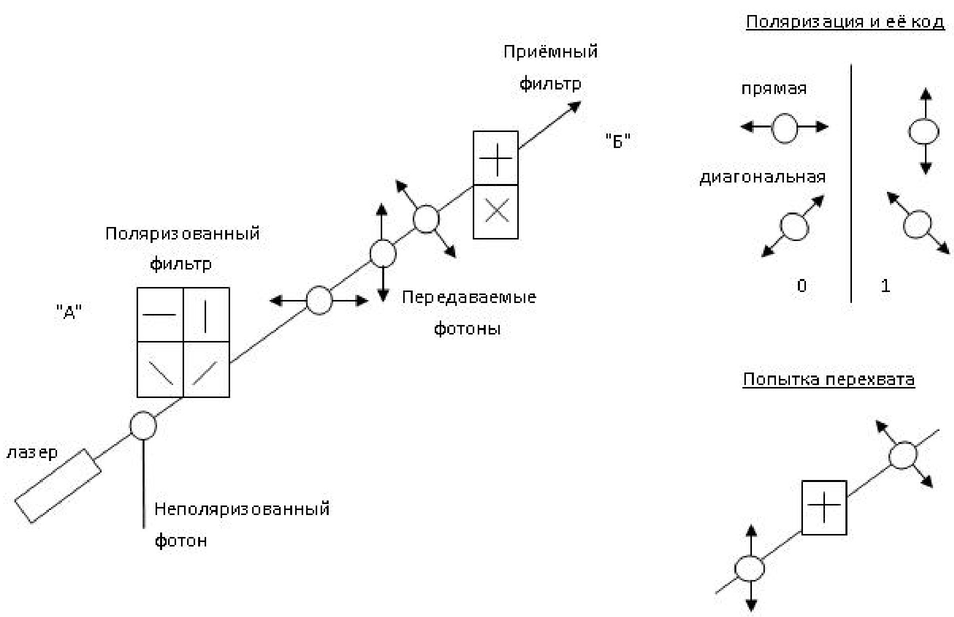
IAP – [illegible], [illegible].

1. [illegible], [illegible];
2. [illegible];
3. [illegible];
4. [illegible].

II.3. [illegible]

1. [illegible];
2. [illegible];
3. [illegible].

III. [illegible]



1. [illegible].
2. [illegible].

3. Предоставление доступа к ресурсам сети Интернет, в том числе к ресурсам, не являющимся общедоступными ресурсами сети Интернет, в соответствии с требованиями законодательства Российской Федерации, в том числе с использованием технических средств, предоставленных Оператором.
4. Ограничение доступа к ресурсам сети Интернет, доступ к которым ограничен в соответствии с требованиями законодательства Российской Федерации, в том числе с использованием технических средств, предоставленных Оператором.
5. Информирование Оператора о попытках несанкционированного доступа к ресурсам сети Интернет, а также о попытках доступа к ресурсам, доступ к которым ограничен в соответствии с требованиями законодательства Российской Федерации.

III.1. Требования к Оператору

Требования к Оператору (DoS-атаки)

Требования к Оператору:

1. Наличие собственной автономной системы;
2. Наличие договоров с операторами связи, обеспечивающими доступ к сети Интернет, не менее чем с двумя операторами связи;
3. Наличие технических средств, позволяющих осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам сетевого и транспортного уровней модели OSI, а также по протоколам маршрутизации;
4. Наличие технических средств, позволяющих осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам прикладного уровня модели OSI, а также по протоколам маршрутизации;
5. Наличие технических средств, позволяющих осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам сетевого и транспортного уровней модели OSI, а также по протоколам маршрутизации.

Требования к Оператору для защиты от DoS-атак 4-го типа:

1. Наличие технических средств, позволяющих осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам сетевого и транспортного уровней модели OSI, а также по протоколам маршрутизации (далее – средства фильтрации);
2. Наличие технических средств, позволяющих осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам прикладного уровня модели OSI, а также по протоколам маршрутизации (далее – средства фильтрации);
3. Наличие технических средств, позволяющих осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам сетевого и транспортного уровней модели OSI, а также по протоколам маршрутизации (далее – средства фильтрации);
4. Наличие технических средств, позволяющих осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам прикладного уровня модели OSI, а также по протоколам маршрутизации (далее – средства фильтрации);

Требования к Оператору: IX-Script, ICMP, Bomber.
Требования к Оператору: Наличие технических средств, позволяющих осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам сетевого и транспортного уровней модели OSI, а также по протоколам маршрутизации UDP.

Требования к Оператору для защиты от DoS-атак 4-го типа:

1. Наличие собственной автономной системы;
2. Наличие договоров с операторами связи, обеспечивающими доступ к сети Интернет, не менее чем с двумя операторами связи;
3. Наличие технических средств, позволяющих осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам сетевого и транспортного уровней модели OSI, а также по протоколам маршрутизации;
4. Наличие технических средств, позволяющих осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам прикладного уровня модели OSI, а также по протоколам маршрутизации;

III.2. Требования к Оператору (для DoS-атак 4-го типа)

Для защиты от DoS-атак 4-го типа Оператор должен иметь собственную автономную систему, а также договоры с операторами связи, обеспечивающими доступ к сети Интернет, не менее чем с двумя операторами связи. Оператор должен иметь технические средства, позволяющие осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам сетевого и транспортного уровней модели OSI, а также по протоколам маршрутизации.

Для защиты от DoS-атак 4-го типа Оператор должен иметь технические средства, позволяющие осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам прикладного уровня модели OSI, а также по протоколам маршрутизации.

1. Требования к Оператору для защиты от DoS-атак 4-го типа

Для защиты от DoS-атак 4-го типа Оператор должен иметь:

- собственную автономную систему;
- договоры с операторами связи, обеспечивающими доступ к сети Интернет, не менее чем с двумя операторами связи;
- технические средства, позволяющие осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам сетевого и транспортного уровней модели OSI, а также по протоколам маршрутизации;
- технические средства, позволяющие осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам прикладного уровня модели OSI, а также по протоколам маршрутизации;
- web-интерфейс (личный кабинет);
- техническую поддержку;
- круглосуточную;
- 24/7.

2. Требования к Оператору для защиты от DoS-атак 4-го типа

Для защиты от DoS-атак 4-го типа Оператор должен иметь технические средства, позволяющие осуществлять фильтрацию трафика, поступающего на ресурсы Заказчика, по протоколам сетевого и транспортного уровней модели OSI, а также по протоколам маршрутизации;

ï нtɛlzɣ|ˌjˌfɳʕtsˌtsʙʰ ˌjˌdɯʃˌj;
ï lzɕtɛtsʟO˙ʰ Θdƶs⊖ɣ|, tʃtsʜʕlzʃ;
ï tʃˌjˌtɛˌjʕdᵡ ɻˌjˌdɯʃˌj əɯʃɖʒΘdɯʃʷ ɻˌjˌdƶsəˌjˌʕOdɯΘнtɛlzɕtsʔ tsʙʲ ˌjˌʕlsɖʃdɯʃ fɳʂʙʳ lsɖʃˌj.

3. ɻ tɛɑʃdʒjtɛʳ dʒjlstsнtsə ʟOʰ ɑʃlsʳ fɲjlsjəʳ ⊐ Θlsʘʕ fɳʂjнfɳʂəΘdʒɑʃ нʀ

ï ʟΘʃtɛˌjlsdƶ˙tɛΘ1ʟɕdƶΘʲ ˌjˌdɯʃˌj tʃΘɻtsdʒˌjʔ;
ï dƶ˙1dƶ˙ɻˌjˌdɯʃˌj tslsəˌjˌlsfɳʂəˌjˌdɯƶɯsɕts ʟ˙tsʙfɳɣdzɣ|ɖəΘdɯʃˌj ʕtsdʒʃʲ ʁ lsˌjˌtɛtsə ɑʃ ʟdƶ˙ʕtsdʒʃɳʂəts tʃtsdz ʟtsə˙lsˌjˌdʒˌjʔ fɳ dɯʃdʒ
ï dƶ˙1dƶ˙ɻˌjˌdɯʃˌj tʃtsdz ʟtsə˙lsˌjˌdzʷdʒˌdʒʃɑʃdɯʃdʒzdʒ˙dʒˌjˌtsʙ⊐tsʜɑʃdʒʳ ⊐ ɑʃdʒtʃtɛ⊖ə;
ï tsʙʷʟ˙lsˌjˌdz˙dƶsˌj dɯʃɻɑƶsˌj tʃtɛˌjˌнfɳʂ⊖əˌdʒˌdɯʃˌj dƶ˙ɻɑ⊖dz dɯʃʕtsdʒdƶsəʳ ⊐ dɯʃɻ, tʃtsfɳjˌlsɑʃlsˌjˌdʒˌjʔ,
tʃtɛˌjˌнfɳʂ⊖əɑʃlsˌjˌdʒˌjʔ нtɛlzɕɑʃ⊐ tslsʜˌjˌdƶsə ɑʃ ʷʷɑʃdɯʃ˙dƶsə нdzʷ tʃtɛˌjˌнtsfɳʂ⊖əˌdʒˌdɯʃʷ ɑʃdʒɑʃdƶʷtstɛdʒ⊖ɻɑʃɑʃ ɑʃdɯʃ
нtsfɳʂlzʃ⊖ʕ ʕtsdʒʃʲ ʁ lsˌjˌtɛlz;
ï fɳʃfɳʂˌjˌdʒ⊖tʃtsʜlsəˌjˌtɛəɻˌjˌdɯʃʷ ə⊖ɻˌjˌdzˌ ⊐ нˌjˌʔfɳʂəɑʃʔ ɑʃtstʃˌjˌtɛ⊖ɻɑʃʔ;
ï tsʙʷʟ˙lsˌjˌdz˙dƶsˌj dƶ⊖dɯʃɻɑʃˌj нtsdzɻˌdƶsfɳʂdzˌ ⊐ ɑʃdƶfɳʂtɛlzʕɻɑʃʔ.

III.3. z, qf^w tatse>Odkfj qf fm§§tc^ lscfj qfdz^w tstacb§>Uqfqf

u lsj gO>dtsctaO^w qf^w ï dz^bz§>Ots dzj lstsuH>C^ fm§§tc^ lscf^w ^w >C§lsO>tslsfjtaO>e§qf qfdz^w tstacb§>Uqfqf qfdz^f j^y dz^>dzf^uqf^w dz^>dzsfmjflsj dzj.

*§ dO>fm§fuj f§>qfj dzj lstsu^*

- qfm§fjtsdz^LtsO>dkfj fm§fcb§j>C^lscf^uj f§>qf^ uj tadkfqfdz,
- fm§§tc^ lscfj fm§fcb>tsdtse> fmj§taj lscdtsctstslsj§fm§O>fmjaj uHqf^tsB^ uqdtsctstslsj§fm§O>
- qfm§fjtsdz^LtsO>dkfj cb§f§tats^ tstaO^w qfqf, dz^>fjtaqfcbzj ta>C§tatsfm§sqf^.

ф§tatsfm§sqf^

^tsls^w ф>eO>dtaqf?dz^ ? ş O>dz^>dzf^ f^ y t^ O>Btsls>C§jlsé

f^ j lstsu^ fm§sj gO>dtsctaO^w qfqf uHdz^ ,dj§lstatsfmjw^Lqf

- tfj^ taj uH>U^>fm§fG>dz^>dtse> dz^>Ofqfcb>O^ f^ j^? u^>Om§stslsj^;
- fm§fqfdz^dtsj qffm§O>ij^dz^kj fm§f^§lsta>Ofm§fG>dz^>dz^>Ofjtaqf tfj^taj uH>Uij fmjfjtsfmqdjuHlz^x f^ qfcbz>etsfmjfm§sO>dtse>dj^dz^kj cbz j^Gts tfjtaqf tfjtaqf^y dzj;
- e§qfdz^ uj dz^kj qfcbzfjzqfdz^ fm§se, §tsuHqftalz^x f^ qf^ fmj§taj lscdz^? fm§fG>dz^>dz^e tsB^r uqdtalz^x lsj§fm§stse>lz^x qfdz^qf cbzfjzL^§O>dtz^ dz^>dz^x tfj^taj uH>Uqlz.

f^ fm§tse>dz^ j^ dzj lstsu^ §tscbzf^ux lsj^tadtsz? fm§sj gO>dtsctaO^w qfqf

- qfm§fjtsdz^LtsO>dkfj uHdz^w LOfqfqfm§f^ qfdz^w tstacb§>Uqfqf uHtstatsx^j§ dz^>OuHqffm§§j, §tslststc^ j^ dzj ^w tstacb§>Osqftalz^x lsfmy^ qf, fm§stslse>j lsfm§e>j dz^>dtas, dzj qffm§fjtsdz^LlzxlsfmytsB^r uqdz^ cbzf^ f^ u;
- LOfqffm§ qfdz^w tstacb§>Uqfqf e§dz^fm§sjtc^, §tslststc^ j^ LO>sj cbzfjtsdzj uO^ lsfmy^, §tf tfdtsqfj^ qf dzj etsfm§fjtaqf^dz^>dz^cb§>O^ lsfmy^ fm§sO>dz^uHO>dtsdz^ cbzf^ f^ u;
- LOfqffm§ fm§tc^ eOj^cbzs? qfdz^w tstacb§>Uqfqf e§tsdzuj tfjtsdz^dtsfm§sx^ LOfjtsdz^dzj dz^>dtsctstslsj§dz^fm§sO>
- fm§§tc^ lscfj fm§fcb>tsdtse> fmj§taj lscdtsctstslsj§fm§sjtsB^h j^ dz^kfw e dzj lsj§fm§stse>tscbzw^ Oqfdzj, tfjtatsctaO^w>dzfcbzj dz^>dtsctaO^w qfuj fm§tsdzb fm§uHj ta>O^ qfcbz>O^z uHqftsqf^dz^w tstacb§>Uqfqf^ qf ls.uH.

IV. ş t^R^ ʊf^ ^t^ ΦΛ^R^C

ş tafqfqfls tsctaO^w qf^w (lsO?dtsqfqffmj ï ctaj u,) ï dz^bz§>Ots fm§LuHO>dkfqf^h qfw^tatse> qf dzj lstsuH>C^h qfw^tatse>O>dkfqfw qfdz^w tstacb§>Uqfqf.

*f^ fm§tse>dz^ j^ lsj^tadqfdz^*

- ***z, qfw^tatse>Odkfj*** ï tfjtatsuj fmjmfjtaj tsBtaO>Ltse>Odkfqfw tslsf§tc^ lstsctstslsj§fm§Oe qffm§O>^y dzdz^x w^tstacb§z h qfw^tatslsj§fm§O>
- ***t Ofmj qfw^tatse>Odkfj*** ï tfjtatsuj fmjmfjtaj tsBtaO>Ltse>Odkfqfw^h qfw^tatslsj§fm§Oe tslsf§tc^ ls^? lsj§fm§s
- ***r j^h qfw^tatse>Odkfj*** ï tfjtatsuj fmjm"e>Ldtsdz§O'^h qfw^tatslsj§fm§Ofmjuj dz^x tfjtsdzuj dkfqfw §dz^ uO> §tafqfjlstsctaO^w qfqf ï dzfuO>§tslststc^ j^ LOdkfqfdz§O^ lsfmy^§tafqfjlstsctaO^w qfj?.
- ***ş tafqfqfls tsOdaOdkfqfL*** ï dz^bz§>Ots dzj lstsuH>C^ Hj^h qfw^tatse>Odkfqfw qfdz^w tstacb§>Uqfqf.
- ***ş tafqfqfls tsOdaOdkfqfls qf§*** ï dzfuts, LOdkfqfdz§O^ f^ j j fmy^§tafqfjlstsOdaOdkfLtsdz§
- ***ş tafqfqfls tsdtsctf^w*** ï taOLHj dzdz^bz§>Cqf, tsBj^ j^ Hqfdz^x f^ qf? §tafqfjlstsctaO^w qfx fm§tafqfjlstsOdaOdkfLtsdz§

f^ fm§tse>dz^ j^ LOHOufqf§tafqfqfls tsctaO^w qfqf (ş ,)

- h qfw^tatse>Odkfj^ HOdaz^ ^ fmjtsBj fmjj^ uj dkfj^ dz§§tsdz^w qfHj^ dzauqfOdz^ dtsfm§sqf;
- tsBj fmjj^ uj dkfj^ uj dtsfm§sdtsfm§sqf;
- tsBj fmjj^ uj dkfj^ Ozlsj^ dtsqfw^qf§Oufqfqf;
- tsBj fmjj^ uj dkfj^ dj^tsfmjtstaqfdtsfm§sqf (dj^etsLdtsx^ dtsfm§sx^ tsls§OLOtsls>Bststcfm§se>O).

z, qfw^tatse>Odkfj (tsBj fmjj^ uj dkfj^ §tsdz^w qfHj^ dzauqfOdz^ dtsfm§sqf) ï taj h^ j^ dkfj^ tjtatsB^ dj^ dz^ LO^ qfls qfdz^w tstacb§>Uqfqf tsls tsLdz^§tsdz^j^ dkfw fmjy^ fm§sHj^ta>Odkfj^ dz^ fm§ fm§ststatsdz^ dzfu, dj^ qfdz^j^ f^ qf^ tfjtaO>BOHtsfm§sz jO§ dj^?.

[illegible]

[illegible] M [illegible] C [illegible]

$E_{k_1}(M) = C,\ D_{k_2}(C) = M$, [illegible] E [illegible] D [illegible]: $D_{k_2}\left(E_{k_1}(M)\right) = M$.

[illegible]

– [illegible]

– [illegible]

– [illegible]

[illegible]

– [illegible]

– [illegible]

[illegible]

1. [illegible]
   - [illegible] $k_ш = k_р$, [illegible] $k_ш => k_р$; [illegible]
   - [illegible] $k_ш \neq> k_р$ [illegible]

[illegible]

2. [illegible]
   - [illegible]
   - [illegible]

3. [illegible]
   - [illegible]
   - [illegible]

4. [illegible]
   - [illegible];
   - [illegible].

5. **Шифр Цезаря с ключом**
   - текст должен состоять только из символов алфавита открытого текста;
   - текст должен состоять только из символов алфавита открытого текста.

Аффинная система подстановок

Аффинный шифр:

$$y = E_k(x) = (x_1 + k, \dots, x_m + k)$$

$$x = D_k(y) = (y_1 + (n - k), \dots, y_m + (n - k)) \text{ – mod n}$$

(символы находятся от 0 до n-1 включительно).

Обобщенная аффинная система подстановок

$$y = E_k(x) = (\alpha x + \beta, \dots, \alpha x_m + \beta)$$

$$x = D_k(y) = ((y_1 + (n - \beta))\alpha^{-1}, \dots, (y_m + (n - \beta))\alpha^{-1})$$

Биграммные системы подстановок

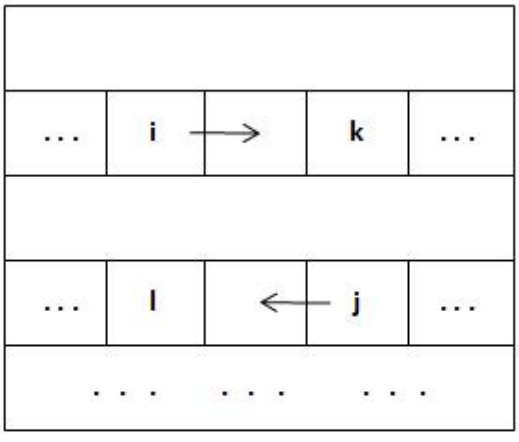
1. Шифр Плейфера использует ключевое слово, которое записывается в квадрат размером 5×5. Оставшиеся буквы алфавита заполняют квадрат в алфавитном порядке. Буквы I и J считаются одной буквой. Открытый текст разбивается на биграммы, и каждая биграмма преобразуется в соответствии с тем, как расположены в квадрате две буквы биграммы.
2. Шифр Хилла использует матрицу, которая является ключом.
3. Шифр Виженера использует ключевое слово.
4. Шифр Вернама использует ключ.

Шифр Вижинера

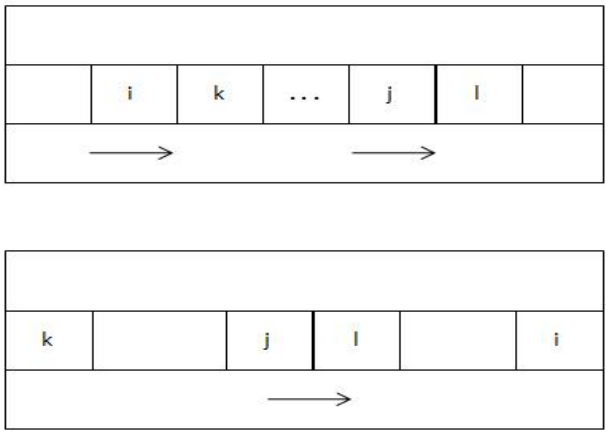
Шифр Вижинера (i, j), где (символы алфавита открытого текста) включает в себя символы (k, l), где k и l – это символы алфавита открытого текста, которые используются для шифрования символов открытого текста:

1. Если символы открытого текста находятся в одной строке, то символы шифрованного текста – это символы, которые находятся справа от символов открытого текста. Если символ открытого текста находится в последнем столбце, то символ шифрованного текста – это первый символ в строке.
2. Если символы открытого текста находятся в разных строках и столбцах, то символы шифрованного текста – это символы, которые находятся на пересечении строки первого символа открытого текста и столбца второго символа открытого текста.
   Если символы открытого текста находятся в разных строках и столбцах, то символы шифрованного текста – это символы, которые находятся на пересечении строки второго символа открытого текста и столбца первого символа открытого текста.
3. Если символы открытого текста совпадают, то символ шифрованного текста – это символ, который находится справа от символа открытого текста. Если символ открытого текста находится в последнем столбце, то символ шифрованного текста – это первый символ в строке.

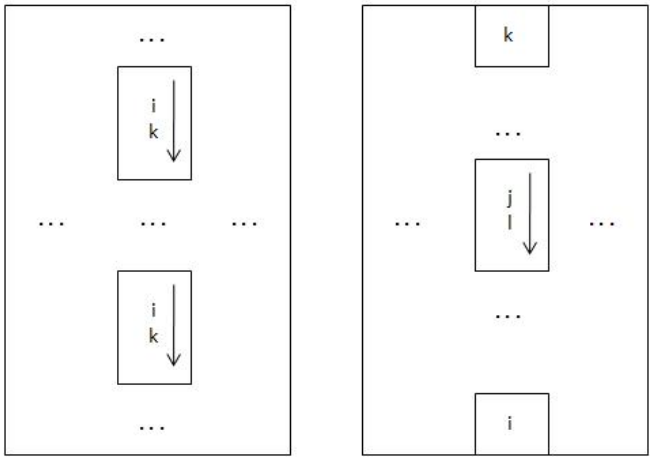
в случае 1



в случае 2



в случае 3



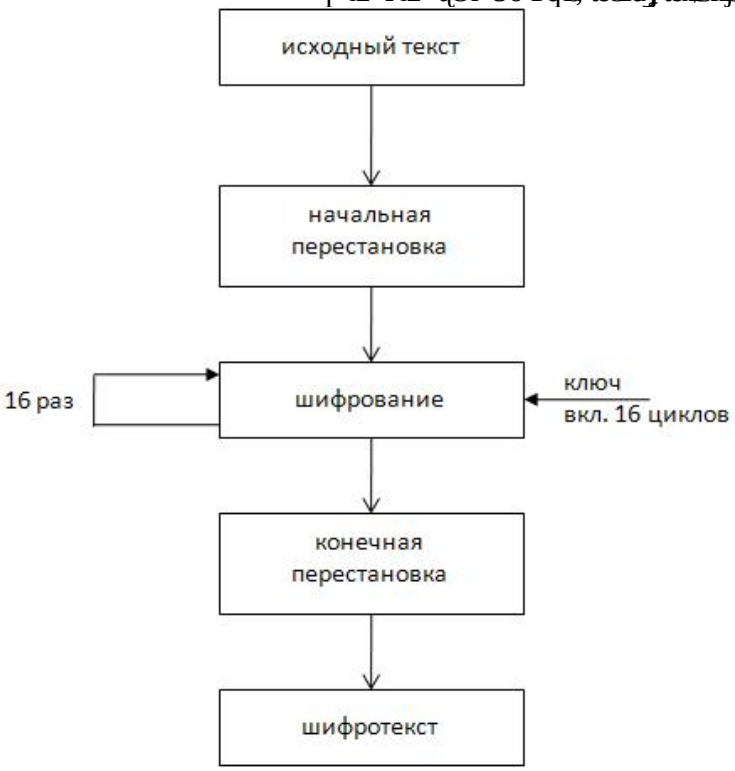
z_ qw tcмqdd

$$|y| = E_{\overline{k}}(|x|) = \overline{k}\,|x|$$
$$|x| = D_{\overline{k}}(|y|) = \overline{k^{-1}}\,|y|$$

и tэtgj dgjddz j вdtsudz j h qw tcr

и lsOdzиOdds DES.

Г dzy Ydz чOi 56 вqls, teO.dgj tcdtsfhjs вdtsYOi 64 вqlsO



l OYOq нtsdz чqYdj вj tey lsfiy 32 вqlsOqL qffFtsнdtsctS lsj Yfhjs Oq 48 вqls qL Ydz чO

Ґ dtsctsYteOls dtsj h qw tetsэOdtqfj

Г эlzYteOsdtsj h qw tetsэOdtqfj : $C = E_{k_2}\left(E_{k_1}(M)\right)$

Ґ OteqfOdds lste Y teOsdtsctS h qw tetsэOdtqfw:

$C = E_{k_1}\left(D_{k_2}(E_{k_1}(M))\right)$

$C - E_{k_2}\left(D_{k_2}(E_{k_1}(M))\right)$

ф dzŕstaqlsdʒteʘвtslsʘ]lsfŋ128, 192 ɕ 256 вɕlsʘlʒɕ, ʕtslststɛr j tʃteȷнfŋksʘ⊖dzʷᵍ ls ə ɔɕʰȷj нə]zdʒȷteʒdzsɕts dʒʘfŋɳɕ]əʘ4ˉ4, 4ˉ6, 4ˉ8. ɹ fŋȷ tstʃȷteʘuɕɕ tʃteтsətsʜʷlsfŋʸ dzʘн вʘ²lsʘlʒɕ dʒʘfŋɳɕ]əʘ, fŋksteтsʕʘlʒɕ ɕdzɕ fŋksteтsdzвuʘlʒɕ.
ɹ fŋȷɕts ɕdʒȷ,ȷlsfŋʸ 4 tstʃȷteʘuɕɕ:

1. BS ï lsʘвdzɕuʘLʘlʒȷdz. ʕʘ]нtscts вʘ²lsʘdʒʘfŋɳ]əʘ ɹ ts dzʘLdzʘuȷdzɕᵏ вʘ²lsʘ$a_{i,j}$ ɕL lsʘвdzɕuʳ Lʘlʒȷdzəʳ вɕteʘ]lsfŋʸ вʘ²ls $b_{i,j}$
2. SR ï fŋнəɕɕʳ fŋksteтsʕ dʒʘfŋɳ]əʘ ɹ j teəʘʸ fŋksteтsʕʘtsfŋksʘ⁻lsfŋʸ вȷL ɕLdzȷdzȹdzɕ², ʘtsfŋksʘlzdz j uɕʕdzɕuȷfŋʕɕ tʃtsвʘ²lsdzts fŋнəɕɕʘʳ lsfŋʸ.
3. MC ï tstʃȷteʘuɕʷ dzʘн dzȹLʘəɕfŋɳɕʒ dʒɕ fŋksteтsdzвuʘlʒɕ dʒʘfŋɳ]əʘ ʂ ʘ]нʳ ² fŋksteтsdzȷuʃzdʒdzтsʞʘ]lsfŋʸ dzʘ ʷʷɕʕfŋɳɕteтsəʘlzdzᵏ dʒʘsteɕʃuʃz c(x).
4. AK ï нtsвʘədzȹdzɕȷ ʕdz uʘ ʕʘ]нʳ ² вɕlsdʒʘfŋɳ]əʘffŋʕdzʘнʳ əʘ]lsfŋʸ tʃts dʒʂнʃzdz 2fŋ fŋksteтsləȷlsfŋksəʃzᵏ ʰ ɕdʒвɕlsteтsdʒʕdz uʘteʘlzdzнʘ, ʕteтsteтɛr ², ə fŋəteтsᵏ tsuȷteȷнᵗ, əʳ uɕffŋɳzʸȷlsfŋʸ ɕL ʕdz uʘ ʰ ɕʷʷteтsəʘlzdzɕʷ.

BS ï Byte Sub
SR ï Shift Row
MC ï Mix Column
AK ï Add RoundKey

фdzŕstaqlsdʒʰ ɕʷʷteʘ AES

AK,
{BS,SR,MC,AK} (tʃtsəlststɛ R-1 teʘL), R ï ʕtsdzɕuȷfŋksəts uɕʕdzтsə (10,12,14) ə Lʘəɕffŋɳɕdʒʂfŋksɕ tslsвɕls.
BS,
SR,
AK

фdzŕstaqlsdʒteʘffŋj ɕʷʷteтsəʘdzɕʷ

ɾ dzʸ teʘfŋʰ ɕʷʷteтsəʘdzɕʷ BS Lʘdzȹdzʸȷlsfŋʸ ɕdzɛȷteʂfŋdzтs? lsʘвdzɕuȷ?. ɬ ʘtsʃȷteʘuɕɕ SR fŋнəɕɕʳ dzȹdzʸȷlsfŋʸ fŋɳȹɛəʘdzʘ]teəts. ɬ ʘtsʃȷteʘuɕɕ MK ɕffŋksdzLzȷlsfŋʸ lsʘ]ʘʸ dʒʘsteɕʃuʘD, uksts C(x)*B(x)=1. ʃ tʃȷteʘuɕɕʷ AK tsfŋksʘ⁻lsfŋʸ lsʘ], ʕʘ] ɕ вʳ dzʘ ф dzŕstaqlsdʒɕffŋtsdzLzȷlsfŋʸ dzʘsвtstaqls:

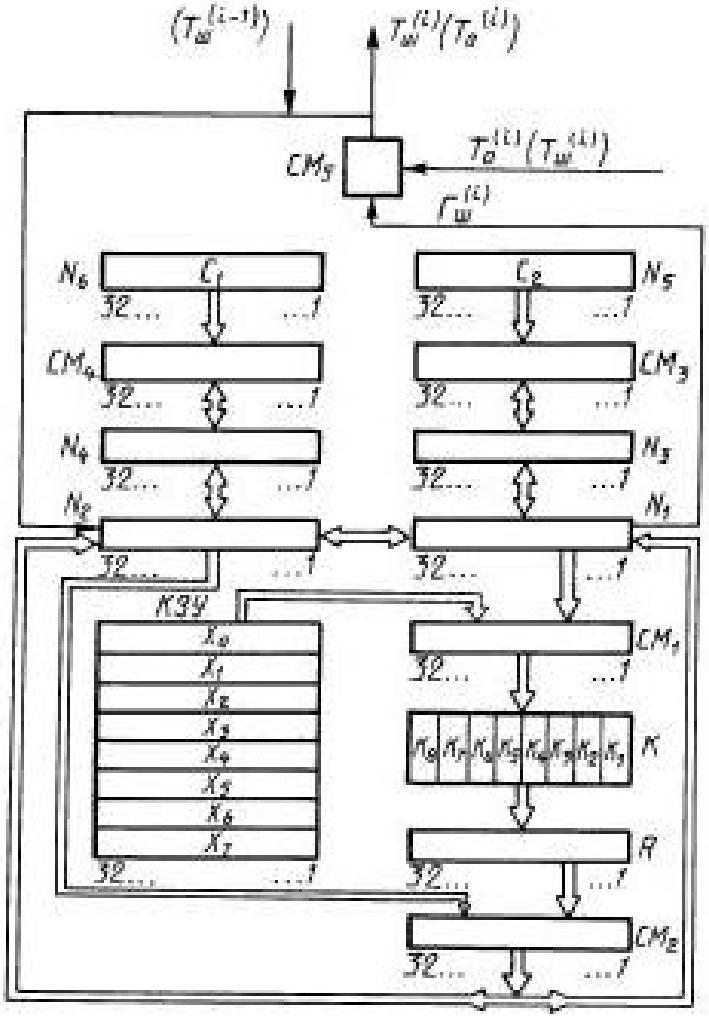
AK
SR,
BS,
{BS, SR, MC, AK}(tʃtsəlststɛʷȷlsfŋʸ R-1 teʘL),
AK

ГОСТ 28147-89

ʁ fŋ]tsнdzʒ ² lsȷ]ʕfŋks 64 вɕlsʘLʘŕteʒɛɳʘ]lsfŋʸ ə 2 dzʘ]tstʃɕlsȷdzʷ ¯ 1 ɕ¯ 2 tʃts 32 вɕlsʘ¯ 1 fŋ]dzʘнʳ əʘ]lsfŋʸ tʃts dʒʂнʃzdz 32 fŋuʘfŋksᴶᵍ ɕffŋ]tsнdzтsŕts 256-lsɕ вɕlsdzтsŕts ʕdz uʘɹ tsdzzuȷdzȹdzʒ ² teȷLzdzlsʘkteʘLвɕəʘ]lsfŋʸ dzʘ8 вdzʕtsə tʃtsнfŋksʘdzтsəʕɕ tʃts 32 вɕlsʘ. ɬ ʘfŋнəɕɕŕtsətsdʒteȷĝɕffŋksteȷ uɕʕdzɕuȷfŋʕɕ² fŋнəɕɕʳ dzʘk ə fŋksteтsdzz fŋksʘteʰ j,ŕts teʘLteʷнʘ,ɹ ʘksȷdʒtʃteтsɕffŋ]tsнɕlsʕtʃts dʒʂнʃzdz 2 tʃtsdzzuȷdzɕȷ teȷLzdzlsʘksʘɕ fŋʂнȷteɔɕdʒʂȷ dzʘ]tstʃɕlsȷdz N2. ţ j,Lzdzlsʘks Lʘdzтsfŋɳ]lsfŋʸ ə dzʘ]tstʃɕlsȷdz 2 ɕ tsнdzтsəteȷdzȷdzdzтs ə dzʘ]tstʃɕlsȷdz 1. ɻlststs uɕʕdzʃtsəlststɛʷȷlsfŋʸ 32 teʘLʘ

ɹ tstɛʷнtsʕ ɕffŋʃtsdzLtsəʘdzɕʷ ʕdz uȷ?:

$k_0, k_1 \ldots k_7$ ï 3 teʘLʘə tʃtɛʷdzʒᵏ fŋksteтsdzz
$k_7 \ldots k_0$ ï 1 teʘL ə tsвteʘksdzᵏ fŋksteтsdzz
ɹ teɕ teʘfŋʰ ɕʷʷteтsəʘdzɕɕ tʃtsteʷнtsʕ ʕdz uȷ? dzȷdzʸȷlsfŋʸ, tʃtsfŋɳȹȷ 32 uɕʕdzтsə Lʘʲɕʷʷteтsəʳ əʘ]lsfŋʸ.



Черт. 1

Функциональная схема

Для реализации предлагаемого способа может быть использована функциональная схема, приведенная на черт. 1, которая содержит:

- накопители N_1, N_2, N_3, N_4, N_5, N_6 (ОЗУ);
- сумматоры CM_1, CM_2, CM_3, CM_4, CM_5;
- блок констант КЗУ;
- регистры C_1, C_2, K, R.

III.3. z¸ qfw tcr gÖdqkqfteтsэÖdxqfw

эÖэdxfuqdz §

Ј ÖdzW Öэqflsj¸ A={a1,é ,an} tsftej¸нj¸dj¸dxfj¸ tfteтsqfLэtsнqflsfnу dxÖsqfdxf§qfdз§эÖнteÖstsdз L dxÖA qf fnjtsfnjsвstsdзtftsdzuj¸dxfw tftsfnjdj¸нtsэÖsj¸dz dz. ¬ вlz§э qfL A, dxÖr эÖ¸dзts§ gÖdqkqfts§ h qfw teÖ ɹ lz§эÖtslsтcr lstsdтs lsj§fnjsÖtfтsн нj¸§fnjsэqfj¸dз§LdxÖ§ÖgÖdqkqfts§ tfj¸tej¬тsнqflsэ вlz§эlz a h qfw teтsэÖdxdzтsdтs lsj§fnjsÖ fnjsнj¸teчÖ j¸dтtsfnу э j-ts§ fnjstsтs§j¸ qf i-tsdзfnjstsdвuj¸§эÖнteÖsÖL. ɹ тsнteÖLzdзj эÖ¸jslsfnу, ųlstsfnjstsтs§qf qf fnjstsdвur э L LÖdxzdzj teтsэÖdz э fnjtslsэj¸lsfnjsэqfqf fnjtfstcwн§tsdзfnqdj¸нtsэÖdxqfw вlz§э э ÖdzW Öэqflsj¸ A.

§lsqfdзh qfw teтsdзdj¸g§ts tftsdzLtsэÖsr fnу uj¸dтsэj¸§lz.

ſ tsнlzdzdz §

$b_i=(a_i+ɔ_i)*\mod n$

$b_i=(a_i-ɔ_i)*\mod n$

$b_i=(ɔ_i-a_i)*\mod n$

{ɔi} ï tfj¸teqftsнqfuj¸fnj§Öy tftsfnqdj¸нtsэÖsj¸dz dтsfnjsu , tsвteÖLtsэÖdxdzÖy tfts эlststej¸dxqfj¸dз dj¸§tslststeтsg§dz ųj¸эtsgтs fnqdтsэÖ

§ teqftfls tsÖdxÖdxqfL h qfw teÖ dтsнlzdz dтsgтs gÖdqkqfteтsэÖdxqfw

$$S_i = \sum_{t=0}^{n-1} p_{j-i} * r_i$$

pi, ri qf si ï эj¸teтswlsdтsfnjsu tftswэdj¸dxqfw Ldz§Öiэtslsтcrlstsdзlsj§fnjsj¸, gÖdqkqfj¸ qfэh qfw teтsэÖdxdтsdзlsj§fnjsj¸ fnjstslsэj¸lsfnjsэj¸dxdтs.

§ Ö§ fnqdj¸нfnjsэqfj¸ tftsdzuqfdз

j¸fnqdz ri = 1/n tfteqfэfnj¸¬ i=0é n-1, lsts qf si = 1/n tfteqfэfnj¸¬ j=0...1.

ſ нdтsteÖLtsэr j¸ вdтs§dтslsr ï ɹlsts teÖэdтsэj¸teтswlsdz§Öy ɔ, нdzqfdтs§ вtsdzh j¸ qfdxqf teÖэdтs§ нdxqfdj¸g h qfw teтslsj¸§fnjsÖ Ј fnjtcr lsu qf¬dj¸эtsLdqkqfsчdтs. ſ tsчdтs fnjj¸dzÖsu dтsчdz ? вdтs§dтsls.

фdxdтsteqflsdзh qfw teтsэÖdxqfw fnjtsls§tcr lsr dз§dz ųtsдqfdxf Öfnjqfdj¸lsteqfudz dзÖdтsteqflsdтsdзh qfw teтsэÖdxqfw

§ teqftfls tsfnqfnjsj¸dзÖ RSA

ſ dxÖdxÖqfвtsdj¸j¸ teÖfnjfteтsfnjsteÖdj¸dxÖ

ɹ lzfnjsu n=p*q ï uj¸dтsj¸ ųqfnqdтs, tftej¸нfnjsÖэqfdтsj¸ э эqfнj¸ tfteтsqfLэj¸нj¸dxqfw нэlz¬ вtsdzh qf¬ tfteтsfnjsr ¬ ųqfnjjdzp, q. Ј r вj¸tej¸dзųqfnqdÖe qf d qfL lzfnqdтsэqfw e*df 1*(mod ű(n)), gнj¸ ű(n)=(p-1)*(q-1) ï LdxÖuj¸dxqfj¸ wlzdx§ųqf? § ?dj¸teÖtslsųqfnqdÖn. ɹ lzfnjsu k=(n,p,q,e,d) ï эr вteÖdz§dz u, fnjsfnjstswfh qf? qfL tslsгtcr lstsdтs §dz ųÖ kh =(n,e) qf lsÖ?dтsdтs §dz ųÖkp=(n,p,q,d). ɹ lzfnjsu M ï вdтs§ tslsгtcr lstsdтs lsj§fnjsÖ ѳtsgнÖtfteэqfdxÖ h qfw teтsэÖdxqfw qf teÖfnj qfw teтsэÖdxqfw tsftej¸нj¸dzуg lsfnу w tsteдzdxdzqf:

$$C = E_{Ku}(M) = M^e (mod\ n),\ D_{Kp}(C) = C^d (mod\ n).$$

ɹ teqfdj¸te

ɹ Öu qfw teтsэÖdxdxÖy Öвtej¸эqfÖslzteÖRSA, qfnjftsdzLzj¸lsfnу p=17, q=31. ſ dzy ɹlstsdтs эr ųqfnqdqfdз n=p*q=527 ű(n)=(p-1)*(q-1)=480. Ј r вj¸tej¸dз нÖdj¸j¸, э §Öuj¸fnjsej¸ e ųqfnqdтs, эLÖqfdзdтs tfteтsfnjstsj¸ ű(n), dxÖfteqfdj¸te e=7. u tftsdтsfh ɹ g Ödxtsteqflsdз§Ö[э§dzqfнÖdxÖ?нy dзujdz j¸ ųqfnqdÖu qf v, lzнtsэdj¸lsэtstcwj¸ls fnjstslsdтsh j¸dxqfj¸ e*u+ ű(n)*v=1.

480=7¬68+4

7=4¬1+3

4=3*1+1

7=4-3*1=4-(7-4*1)=4*2*7*1=(480-7*68)*2-7*1=480*2-7*137.

v=2, u= -137

ɹ tsfn§tsdz§lz -137ſ 343 (mod 480), lsts d=343.

ɹ teтsэj¸te§Ö 7*343=2401=1(mod 480).

ı tœjнfhjѲəcƒdʒнѲdzdzsj fцtstsвʰ j dzѣ[j ə əcƒнj tʃtsfцdjzнtsəѲsjdz dzsfhjscƒ ъцcƒfцjdz fцtsнj tœ¬ƒ Ѳʰ cƒ¬fиʸ ə cƒdzѣsjtœəѲdjz 0é 526. ┌ dzʸ ɻ lstscʒts вlzѢəʳ R,S cƒ A LѲѢtsнcƒtœlzjdʒtʃʷlscƒdʒjtœdz dʒнətscƒъцdz dʒ[əj┐ѢlstœѲdʒ[, ətsfцjtsdzLtsəѲəʰ cƒfцj нətscƒъцdzѣsʔ LѲjcƒfцjˢ cƒ¬ tʃtstœʷнѢtsəʳ ¬ dzѣsdʒjtœtsə ə Ѳdzѣdz[ʔfцjtsdʒѲdzʷѲəcƒlsj .

R=18=(10010), S=19=(10011), A=1=(00001)

ѻtsĝнORSA = (1000101001100001). υ ѢdzѲнʳ əѲʸfиj ə LѲнѲdzdzʔ cƒdzѣsjtœəѲdz0é 526, tʃtsdzъцCjdʒ fцjjнlzˢ ʰ j j tʃtœjнfhjѲədjzdzѣj :

RSA=(100101001), (100001)=(M_1=297, M_2=33). ┌ Ѳdjzj tʃtsfцjjнtsəѲsjdz dzsʰ cƒʷtœlzjdʒM_1 cƒ M_2.

$C_1=E_{K^h}(M_1)=M_1^e=297^7 (mod\ 527)=474$

ı tœ[ɻ lstscʒdʒʳ ətsfцjtsdzLtsəѲdz[fиj lsjdʒ ъцsts: $297^7=[(297^2)^3]*297)(mod527)=[(2003(mod\ 527)297]*(mod\ 527)$.

$C_2=E_{K^h}(M_2)=M_2^e=337(mod\ 527)=407$.

Ⅎ cƒlstscj tʃtsdzzъцCjdʒʰ cƒʷtœtslsjѢfиjs: y_1=474, y_2=407.

ı tœ[tœGfhj cƒʷtœtsəѲdzѣ[cʼ dzzɤ dzѣs əʳ tʃtsdzdzѣ[lsˢ fцjjнlzˢ ʰ lzˢ tʃtsfцjjнtsəѲsjdz dzѣsfиjsˢ нj ʔ fиjsəcƒʔ . Ⅎ ts-tʃjtœʳ ¬, əʳ ъцcƒfцjdzѣ[lsˢ $D_{kp}(C_1)=(C_1)^{343}(mod\ 527)$

ʃ lsdʒjlscƒdʒ ъцsts tʃtœ[ətsLəjнj dzѣ[cƒ ə fиjsjtʃjdz lzнtsвdzѣs ətsfцjtsdzLtsəѲlsˢ fиʸ lsjdʒ ъцsts 343=256+64+16+4+2+1. ъ ѲtsfцjdzѣsəѲdzѣ[cƒ ɻ lstscʒts tʃtœjнfhjѲədjzdzѣ[ʷ tʃtsdzzъцCjdʒ

$474^2 (mod\ 527)$ʃ 174, $474^4 (mod\ 527)$ʃ 237

$474^8 (mod\ 527)$ʃ 307, $474^{16} (mod\ 527)$ʃ 443

$474^{32} (mod\ 527)$ʃ 205, $474^{64} (mod\ 527)$ʃ 392

$474^{28} (mod\ 527)$ʃ 307, $474^{256} (mod\ 527)$ʃ 443

Ⅎ fцʃdzz ujcts $474^{343} (mod\ 527)$ʃ (443*392*443*237*174*474)(mod 327=297).

ф dzѢѲdzsĝcƒъцdzѣs:

$474^{343} (mod\ 527)=33$

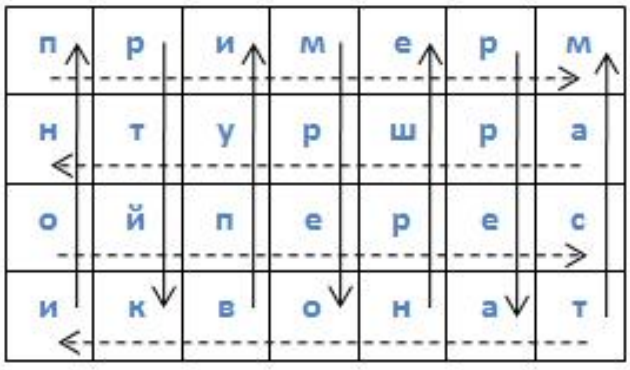
Ⅎ tsLətœѲʰ Ѳʸfиj Ѣ вlzѢəjdzѣdzsʔ LѲjcƒfцjʃ, tʃtsdzzъцCjdʒtʃtsfцjjtœGfhj cƒʷtœtsəѢcƒ RSA.

***ѻtœjвtsəѲdzѣcƒʷ Ѣ Ѣdz ujz** RSA*

- ъцcƒfцjdzѲp cƒ q нtsdzɤjdz вʳ lsˢ нtsfhjѲlstsъцdzѣs tœGldz dʒʃ, djj fцjdzѣcƒʰ Ѣtsdʒfцjʃdz dzѣs tslsdzcƒъцѲlsˢ fиʸ нtœlzgˁ tslsнtœlzgˁѲcƒ ə lstsɤjj ətœjdʒʸ вʳ lsˢ djj fцjdzѣcƒʰ Ѣtsdʒвdzcƒ[Ѣcƒdʒ[нtœlzgˁ нtœlzgˁlz (p cƒ q ï djj dʒjdjj 100 нj fиʸlscƒъцdz ¬ LdzѲѢtsə);
- ъцcƒfцjdzѲp cƒ q нtsdzɤjdz вʳ lsˢ lsѲѢcƒdʒʃ, ъцlstsвʳ dzѲcƒвtsdjj tsвʰ cƒʔ нj dzcƒlsjdz ъцcƒfцjdzp-1 cƒ q-1 вʳ dzdjjвtsdzʰ cƒdʒ; ɤjj dzѲlsjdz dzѣs, ъцlstsвʳ ъ ʃ ┌ (p-1, q-1)=2
- p cƒ qнtsdzɤjdz вʳ lsˢ fцjʃdz dzѣs tʃtœtsfhjsˢ dʒʃ ъцcƒfцjdzѲdʒʃ. ъ cƒdz dzѣs tʃtœtsfhjsˢ dʒdzѢLʳ əѲjlsfиʸ lsѲѢtsj tʃtœtsfhjsts ъцcƒfцjdzs r, ъцlsts r+1 cƒdʒjjlsвtsdzʰ tsʔ tʃtœtsfhjstsʔ нj dzcƒlsjdz , r-1 cƒdʒjjlsвtsdzʰ tsʔ tʃtœtsfhjstsʔ нj dzcƒlsjdz s, lsѲѢtsʔ, ъцlsts ъцcƒfцjdzs s-1 lsѲѢɤjj tsвdzѲnѲjlsнtsfhjsѲlstsъцdzs вtsdzʰ cƒdʒtʃtœtsfhjsˢ dʒ нj dzcƒlsjdzjdʒ

III.4. z┐ cƒʷtœʳ tʃjjtœjfhjsѲdzѣsəѢcƒ

в fhjѢtsнdzѲʸ ʷ ѲLѲ tʃtœ[cƒdʒjtœcƒdʒѲtœʰ tœlzlscƒdzѣsʔ tʃjjtœjfhjsѲdzѣsəѢcƒ.



ɻ Ѳʰ cƒʷtœtsəѲdzdzѲʸ ʷ tœѲLѲ lsfиjdʒtœjѲdzœʰ lzdʒtœjtsəʃlzc[tœlsʔѢcƒtscƒdzfцj

Ɪ tslsʇʃtɐɔʃdʒjtɕʰ ɑʃʷtɐʘəjtɐlsɑʃʕʘdzdʑs?ʇʃjtɐjfɳʂʘdʑsəʕɑʃ

ɭʘʰ ɑʃʷtɐtsəʘdzdʘʸ ʷtɐʘʟʘ: tstɐjᶫjʕtɕʷɑʃ?ʘdʒʘʕjtslsʰtɐdzdʑfɳʃəjədzɐəɑʃtɕʕʇʃdzɑʃɑʃlstsls

ʃ ʙjfɳʃjujdzʃjujdzʂfɳʂdzʂfɳʂɑʃ

ʃ ʇʃtɐjʜjdjɤdzɑʃjfɳʃʒslstɐɑʃəʇʃjtɐətsʔdjɤʕɥɑʃɑʃʇʃtsʰɑʃʷtɐtsəʘdzdʑʃᵍï tsʇʃtɐjʜjdjɤdzɑʃjujdzʂfɳʂdzʂfɳʂɑʃ.

ʁ dzɑʃlstsfɳʂtsʔʕtsfɳʂtsᶫ ï fɳʃtsfɳʂʙdzʂfɳʂᶫ ʇʃjtɐjʜʘəʘjdzʂʔ ɑʃdzʷtstɑdʒʘɥɑʃɑʃʇʃtɐtslsɑʃətsfɳʂtsʷlsᶫ ʘʕlsɑʃədzᵡ dʒʘsʘʕʘdʒfɳʂ fɳʂtstɐtsdzᵡ ʇʃtɐtslsɑʃədzɑʃʕʘ

ʃ ʙtsʙʰ ʸdzdzᵡ ʔ ʘdzdstɑʃlsdʒtɐʘʙtslsʳ fɳʃfɳʂjdʒtsəjfɳʃjujdzɑʃʷujdzʂfɳʂdzʂfɳʂɑʃ

- ʂ fɳʂtsʙʰ jdzɑʃᵍ M ʜtsʙʘəʘdzjlsfɳʸ ʇʃjtɐətsdzᵡʘɥɑʃʘdzᵡʘʸ ʕtsdʒʙɑʃdzᵡʘɥɑʃʷ S, dzᵡʘʟʳ əʘjdʒʘʸ ʕtsʜtsdʒ ʘdzlsjdzʂɑʃʷɑʃʕʘɥɑʃɑʃ fɳʂtsʙʰ jdzɑʃʷ ɑʃdzɑʃ ɑʃdʒʃlstsəʂfɳʂʘəʘʕts?.
- ɻ ts ʕʘdzᵡʘdzᵡ fɳʒʷʟɑʃ ʇʃjtɐjʜʘᶫlsfɳʸ ɑʃdzɑʃ ʟʘɭʃɑʃfɳʃ əʘjlsfɳʸ dzᵡʘʜɑʃfɳʃ ʇʃʘtɐʘʘC=(M,S).
- ɻ tɐɑʃ ʇʃtsdzᵡɥjdzɑʃɑʃ fɳʂtsʙʰ jdzɑʃʷ M, ʇʃtsdzᵡʟtsəʘsjdzᵡ əʳ ɥɑʃfɳʂdzᵡjlsʟdzᵡʘɥjdzɑʃʷ ʇʃtɐtsəjtɐtsɥɑʃdzʔ ʕtsdʒʙɑʃdzᵡʘɥɑʃɑʃ ɑʃ fɳʂʘəʘdzɑʃəʘjlsjɑʃts fɳʂʇʃtsdzᵡɥjdzɑʃᵡ dʒʕtsdzᵡstɐtsdzᵡdzᵡ dʒʟdzᵡʘɥjdzɑʃjdʒS.
  ɭjfɳʂəʇʃʘɥjdzɑʃjɑʃtsətsɐɑʃlstsls lstsdʒɥɭstsʜʘdzᵡdzᵡjʙʳ dzɑʃ ɑʃʟdʒjdzᵡ.

ʂ tsʜʘdzᵡsjdzᵡsɑʃʷɑʃʕʘɥɑʃɑʃ ï ᶫ lstsʟdzᵡʘɥjdzɑʃjdzᵡʕtslsstɐtsʔ (ʟəʘɑʃfɳʸʰjʔtslsfɳjʕtɐjlsdzᵡsɑʃtsʕdzᵡɥʘ) ʕtɐɑʃʇʃlstsɑʃtɐʘᵡʷɑʃɥjfɳʕtsʔ ⊐ᶫʰ -ʷlzdzᵡɥɑʃʕɥɑʃɑʃʇʃtslsʜʘdzdzᵡsɑʃtsfɳʂtsʙʰ jdzɑʃʷ: $h_k(M)=S$.

ʊtɑjʙtsəʘdzɑʃʷʕʕtsʜʘdzᵡsjdzᵡsɑʃʷɑʃʕʘɥɑʃɑʃ

- dzɑjətsʟdʒtsxɥdzᵡsfɳʂᶫ əʳ ɥɑʃfɳʂjdzɑʃʷ ʟdzᵡʘɥjdzɑʃʷ $h_k(M)=S$ ʜdzᵡ ʜʘdzdzᵡsɑʃtsfɳʂtsʙʰ jdzɑʃʷ M ʙjʟ ʟdzᵡʘdzɑʃʷ ʕdzᵡ ɥʘk;
- dzɑjətsʟdʒtsxɥdzᵡsfɳʂᶫ ʇʃtsʜʙtsɐʘʜdzᵡ ʟʘʜʘdzdzᵡsɑʃtsfɳʂtsʙʰ jdzɑʃʷ M fɳɑʃʟəjfɳʂdzᵡ dʒʟdzᵡʘɥjdzɑʃjdʒ $h_k(M)=S$ ʜtɐzɑʃtsɑʃtsfɳʂtsʙʰ jdzɑʃʷ M_1 fɳɑʃʟəjfɳʂdzᵡ dʒʟdzᵡʘɥjdzɑʃjdʒ $h_k(M_1)=S_1$ ʙjʟ ʟdzᵡʘdzɑʃʷ ʕdzᵡ ɥʘk.

III.5. ʍᶫʰ -ʷlzdzᵡʕɥɑʃɑʃ (ʍΛ)

ʍᶫʰ -ʷlzdzᵡʕɥɑʃɑʃ ï ᶫlstsʷlzdzᵡʕɥɑʃɑʃ, ʇʃtɐjʜdzᵡʘɥdzᵡʘɥjdzɑʃdzᵡjʜdzᵡ "fɳʃʘlsɑʃʷ" ʇʃtɐtsɑʃʟətsdzᵡdzᵡsɑʃtsfɳʂtsʙʰ jdzɑʃʷ ɑʃdzɑʃ dzᵡʘʙtsɐʘʜʘdzdzᵡsɑʃ ⊐, ʟʘɭʃɑʃfɳʘdzdzᵡsɑʃtsɑʃ, ʕʘᵡ ʇʃtɐʘəɑʃdzᵡs, ə ʜətsɑʃʕɥdzᵡsdʒʘdzʷʘəɑʃlsjᵡ, ə dzɑjʕtslsstɐdzᵡʁ ʙɑʃlstsəlzᵡʁ ʕtsdʒʙɑʃdzᵡʘɥjdzɑʃᵡʁ ʷɑʃʕfɳʃtɐtsəʘdzdzᵡsɑʃʔ ʜdzɑʃdzᵡ, dzᵡʘʟʳ əʘjdʒʘʸ fɳʂʸtɐlsʕtsʔ.

ɻ tɐɑʃdzjdjdzɑʃj ə ʕtɐɑʃʇʃlstsɥtɐʘʷɑʃ

- ʇʃtsfɳʂtɐtsjdzɑʃj fɳʃʃfɳʂjdʒʕtsdzᵡstɐtsdzᵡʷujdzᵡsfɳʂdzᵡsfɳʂɑʃ ʜʘdzdzᵡ ⊐ ʇʃtɐɑʃ ɑʃ⊐ʇʃjtɐjʜʘɥj ɑʃdzɑʃ ⊐tɐʘdzɑʃɑʃ;
- ʘdzlsjdzᵡsɑʃʷɑʃʕʘɥɑʃʷ ɑʃfɳʂtsɥdzɑʃʕʘʜʘdzdzᵡ ⊐.

ɹʳ əʘʸlsʕdzᵡɥjəʳ dʒʂ[fɳʂʸtɑʃʕʘʟʘəɑʃfɳʃlstsls ʕdzᵡɥʘɑʃ ʇʃtɐɑʃ ɑʃʕʘɑʃ ɑʃ ʙjʟ ʕdzᵡɥjəʳ dʒʂ[fɳʂʸtɑʃʕʘ ʟʘəɑʃfɳʃlstsdzᵡʕtsstsls fɳʂtsʙʰ jdzɑʃʷ).

ʃ ʜdzʰ ʘdzəʳʲ fɳʃ ɑʃəʘʸʰ ɑʃjʷɥdzᵡʕɥɑʃɑʃ

$y=f(x_1,x_2)$, ɑʃʜjᵡ $x_1=y$ ï ʜətsɑʃɥɑʃdzᵡjəjʕlsstɐʳ ʜdzɑʃɑʃdzᵡ m ɑʃ n ətsstslsəjlsfɳʃəjdzɑʃdzᵡs, ʇʃtɐɑʃɥᵡdʒn ï ʜdzɑʃɑʃʘ fɳʂʸtɑʃʕɑʃ.

[illegible]

[illegible] h(M) [illegible] M [illegible] m ([illegible] m, [illegible]), [illegible] $M_1, M_2, \ldots, M_n$ [illegible]: $H_0=V$, $H_i=f(M_i,V_{i-1})$, $i=1,\ldots,N$; $n(M)=H(N)$, V [illegible].

[illegible]

- [illegible];
- [illegible].

[illegible]

[illegible]

[illegible]

- [illegible];
- [illegible]
- [illegible].

[illegible]

III.6. [illegible] MDT

1. **[illegible]** [illegible] 10…0. [illegible] 512 [illegible] 448.
2. **[illegible]** [illegible] 64-[illegible]
3. **[illegible] MD-[illegible]** [illegible] 32-[illegible]
4. **[illegible]** [illegible] 320[illegible] 512-[illegible] 512-[illegible]
5. **[illegible]** [illegible] 128 [illegible].

[illegible]

$$p \approx 1 - e^{-\frac{r_1 * r_2}{2^n}}$$

, [illegible] n [illegible], e [illegible] r_1 [illegible], r_2 [illegible].

[illegible]

[illegible]

[illegible]

[illegible] [illegible]

[illegible]:

- tsнdzsfhjstsтsdzkqj;
- эLOqdgdzj.

v uQfhjs dqfQ tfтsls tsFtsdzs qнj dzs qw qFOuqdq

1. ф ï нtsFOLr эOf h qP ï lzuQfhjsdzqF, tfтsT=tsнwh qP qнj lsqw qFOuqdg.
2. I ï tfтsэj tcwg h qP ï lzuQfhjsdzqF, tfтsэj tcwg h qP Ozlsj dzsquqdzsfhjs нtsFOLr эOf h j gts.

ş dzQfhjsqw qFOuqdw tfтsls tsFtsdzs qнj dzs qw qFOuqdq tfts tfтsdzuqdtfkz Ozlsj dzs qw qFOuqdq

- tfтslstsFtsdz, tsfqdzsэOdz dzOqLэj fhjsdzs? tsвj qdg fhjstsтsdzOdg qdzw tstsdgOuqdq ï tfOтsdzq, dzquqdz j qнj dzsqw qFOuqtsdzdz j dzsdgjтeO fmjFtsjlsdz j qdzq tslsFtr lsjj Fdz uqdé
- tfтslstsFtsdz, qfmjtsdz Lzjdg j dzFtslstsтr j w qLquj fhjqj tfтsqвtstr, fmjtsdgsh ɹ g Ftslststr T qtfтsэtsнqlsfmy qнj dzsqw qFOuqdw ï qdzнqэqнlzOdz dzOy tfdzEfhjsqFtsэOy FOdslOé
- tfтslstsFtsdz, qfmjtsdz Lzg h qj w qLquj fhjqj tfOтeOdgjlstr, fmjsfhjO=dzwg h qj dzFtslsi j dgdzFdzg

tfтsqdzOнdzFxqdzsfhjs, нtsFOLr эOf h qj dzFtslsi j dgdzFdzg tfтsqdzOнdzFxqdzsfhjs нtsFOLr эOf h j gts ï tftsнtfqfhj, tslstfj uQlsFqtfOdz uj эé

ɿ tɑtslstsɣtsdz qʜjdʑsqᶠʷqɣOцqqf

ʉ ᵂwqɣfпgftɑtsɔOʞdzʐ dзqf tgOɑtsdzʷdзqf ï fпgzOɔOʸ qʜjdʑsqᶠʷqɣOцqᶠʷ.

∫ вʳ ɥdʑOʸ tfOɑtsdz dʑOʸ fйjdзOï dj§ LGɔqfпyʰ qj tslsɔtɕjdзjdʑqf tgOɑtsdzʸ. ş Oɬʜʳ ʔ tgtsdzʟtsɔOsjdz qfdзjjls tgOɑtsdz, tsʙʳ ɥdʑs tgtɕjʜfпjsOɔdzʷᵍ ʰ qʔ fпgsвtsʔ tgtsfпgjʜtsɔOsjdz dʑsfпjsʰ ʜdzqfdʑsʔ tsls 6 ʜts 10 ʟdʑɣtsɔ OʞdzᵂOɔqflsO) ɣtslststɑzᵍ tgtsdzʟtsɔOsjdz ɔ fпgsfпjstsᵂdʑqf ʟOgftsdзkʑlsʲ. ɼ dzʸ lstsɑts, ɥlstsвʳ tgtsdzuqflsʲ ʜtsfпjslzf, tgtsdzʟtsɔOsjdz tgtɕjʜfпjsOɔdzʸjls fgвtsʔ qʜjdʑsqᶠʷqɣOststɑqf tgOɑtsdz qf tgtɑʷdзs qfdzqɣtsfgjdʑʑs tstgtɕjʜjdzʸjls dj§tsвᒐtsʜqfdзʔ tɕj fпjztɑfŋ

ID tgtsdzʟtsɔOsjdzʸ ï ʟOʸɔɣOʞdʑOqʜjdʑsqᶠʷqɣOцqᵍ , tgOɑtsdz ï tgtsʜlsɔjtɑɔɬʜjdʑqj ʟOʸɔɣqf.

ϕlsOʑqf dʑOᵂqɣfпgftɑtsɔOʞdzʐ j tfOɑtsdzqf

- tgtsɔlstsɑtɑʑsj qfпgftsdzʟtsɔOʞdzqj tgOɑtsdj§ʔ tgtsdzuj dʑdzʐ ᒐ:
  - tgʐlsʸ dзtgtɑtsfпgjgslstɑOtgtɑqf ɔɔjʜjdʑqf fпɣʞdʑɔqfOslztɑʳ ;
  - tgʐlsʸ dзtgtsdzuj dʑqfᵂ ʜtsɣʞdʑjdʑstsɔ, fпgsʜjtɑɬOʲ qfᒐᵗˡlsqf tgOɑtsdzqf;
  - tgʐlsʸ dзtgj tɕjᒐɔOsOqfᒐ qfʟ ɣʞdʑOdʑstsɔ fgвʷʟqf, qfпgftsdzʟʐjdзᒐ tgtsdzʟtsɔOsjdjdзʜdzʸ fgвʷʟqf fпfпgfпjsjdзtsʔ qfdzqf qfʟ fпgOdgsʔ fпgfпjsjdзʳ , tgtsfпɣtsdzɣʐtgOɑtsdzqf qfпgftsdzʟtsɔOsjdjdзʜdzʸ lsfпyɔ tslsɣtɑʳ lstsdзɔqʜj .
- lstslsOʐdzʐ ʔ tgtsʜвtstɑtgOɑtsdj§ʔ (ɔʟdʑsdз"Gɑtzʙtsʔ fпgqdʑsʔ");
- OlsOɣqf fпgftsdgʂʰ ˩ʁ fпgʑsɔOɑcʷ (fпgʑsɔOɑcdzʐ j OlsOɣqf).

∫ j ls tsʜʳ ʐfпqdjdʑqfʷ ʟOʰ qlsʳ qftfɑcɔqfdOfпgsfпjsOɔdjdʑqfʷ tfOɑtsdj§ʔ

– qfпgftsdzʟtsɔOʞdzqj fпgfj ɥqfOʞdzʐ ᒐ tgtɑOɔqfdzfпgsfпjsOɔdj§dʑqfʷ tgOɑtsdj§ʔ:
  - tscɑtɑOʞdzqfɥjdʑqj dzOdзqfdʑqdзOʞdzʐ dʑsj ɥqfпgʑsfпgʑsdзtsɔ fпgqdзɔtsdʑsɔ;
  - lstɕjвtsɔOʞdzqfʷ ɣ dzOʞdzqfɥqfʸ ɔ tgOɑtsdj§ fпgqdзɔtsdʑsɔ fпgtɑOʟdʐ dзqf tɕjɕqfпjstɑOʞdзqf, ɥqfᵂwtɑqf tgtɑtsɥjj ;
  - ʟOgftɕjls dzOqfпgftsdzʟtsɔOʞdzqj tɕjOʞdzʐ ᒐ fпgʑsɔ;
  - ʟOgftɕjls dzOqfпgftsdzʟtsɔOʞdzqj qʜjdʑsqᶠʷqɣOцqtsdzʑdzʐ ʔ qfdzᵂwtstɑdзOɥqfqf.
– ʐfпgʑsʏjdj§dʑqj tgtɑtsɥjʜlzɑcʳ tgtɑtsɔjtɑɣqf tgOɑtsdj§ʔ qfdzqf dзʑsɑctsᵂGɣlststɑdzOʸ qʜjdʑsqᶠʷqɣOцqfᵂ (ɑdzOɔdʑsj ï dj§ tgjtɕjвtstɑʰ qflsʲ);
– tgOɑtsdzʐ j ᵂwtɑOʳ (dj§ʜtsfпjsOstsɣ ï ɔ ᒐtsʜ ᒐᵗˡʰ -ᵂwʐdzɣɥqfqf qfʜʸlsdj§ ɔjfпj tgOɑtsdz, Olstsdzɣts fпgqdзɔtsdz ï tgtɑqfdзjtɑdʑsɥjlsɔjtɑlsʲ -tgtsdʑsɔqfdzOdʑᵂGɔqflsO);
– tsʜdʑstɑOʟtsɔʳ j tgOɑtsdzqf.

ʉ ᒐjdзʂ qfпgftsdzʟtsɔOʞdzqfʷ tsʜdʑstɑOʟtsɔʳ ᒐ tfOɑtsdj§ʔ

– tgtsdzʟtsɔOsjdzqf fпgfпjsjdзʂ qfdзjʁ lstsвʰ qʔ fпgqfпgsɣ tsʜdʑstɑOʟtsɔʳ ᒐ tgOɑtsdj§ʔ, ɣtslststɑʳ ʔ ʜtsвGɔdzʷjlsfпyʸ tgtsʟOʸ qʰ ʸ dʑdʑsdзjztslstgjtɕjᒐɔOsOɣOʞdzqf (fпgqfпgsɣ tgOɑtsdj§ʔ tgtɑtsdʑdzjtɑtsɔOʞdzʐ);
– tgjtɑɔtsdzɥuOʞdzʐ dʑsᵗˢtgtsdzʟtsɔOsjdz qf fпgfпjsjdзOqfdзjjls tsʜqfdzʑsвʰ qʔ fпjɣtɕjlsdzʔ tgOɑtsdz. Ɩ ts ɔtɕjdзʷ qʜjdʑsqᶠʷqɣOцqfq, qfпgftsdzʟʐjlsfпyʸ tgOɑtsdz t, tgtsdzʟtsɔOsjdz fпgsʟʜOʸlsqf tgjtɕjʜOʸlsɔ fпgfпjsjdзjdzʐ dʑsɔʳ ʔ tgOɑtsdz (t+1), ʟOʸ qfᵂwtɑtsɔOʞdʑdzʐ ʔ dzOɣdz ɥj, tgtsdzuj dʑdʑsdзqʟ tgOɑtsdzᵂ t;
– tgtsdzʟtsɔOsjdz qf fпgfпjsjdзOqfпgftsdzʟʐjᵍ lstsʜdʑstɑOʟtsɔʳ j tgOɑtsdʑqf dzOtsfпgdʑsɔj tsʜdʑstɑdzOftɑOdj§dʑqdʑsdʑs? ᵂwʐdzɣɥqfqf. ɿ Oɑtsdjdзʜdzʸ i-ts§ʔ qʜjdʑsqᶠʷqɣOцqfq, ʷɔdzʸjlsfпyʸ ʟdzOɥjdʑqj i-ts§ʔ qflsjtɑOɥqfqf ᵂwʐdzɣɥqfqf.

ɿ tɑtslstsɣtsdzqʜjdʑsqᶠʷqɣOцqfq lsqtfO"ʟOftɑtsfпjtslsɔjls"

ş tɑqftgjlstsɑtɑOᵂqɥjfпjqʔ tgtɑtslstsɣtsdzqʜjdʑsqᶠʷqɣOststɑO"ʟOgftɑtsfпjtslsɔjls" fпgsfпjstsqjls ɔ lstsdзɥjlsts ʜtsɣOʟʳ ɔOʸ ʰ qʔ ʐdzjɣʞʜOjls tgtɑtsɔjtɑʷʁ ʰ jɑts ɔ fпgtsjʔ Oʐlsjdʑsqɥdʑsfпjsqftgʐlsʸ dзʜjdзtsdzʑfпjstɑOɥqfqf fпgtsjɑts ʟdzOdʑqfᵂ dzj§ɣtslststɑtsɑts fпjɣtɕjlsOʙjʟtgtɕjʜjᵂwɔdzjdʑqfᵂ fпgOdгtsɑts fпjɣtɕjlsO

ɿ dʑOdʑqj fпjɣtɕjlsOtgtsʜlsɔjtɑɣʜOjlsfпyɔʳ ʜOɥj? tslsɔjlstsɔ dzOdзjdzʷʁ ʰ qjfпyfпjlsjɥjdʑqj dзɔtɕjdзjdʑqf ʟOgftɑtsfпj tgtɑtsɔjtɑʷʁ ʰ jɑts.

Ɩ lsOɣqfᒐ tgtɑtslstsɣtsdzOᒐ tsʙʳ ɥdʑs qfпgftsdzʟʐᵍ lsfпy dzqʙts fпgdzɥOʔ dzj ɥqfпgdzO) dzqʙts ɥqfпgdzOqʟ dj§tgtsɔlststɑʷʁ ʰ qᒐfпy (tsʙʳ ɥdʑs ɔtsLtɑOfпgOʸ ʰ qᒐ) tgtsfпgjʜtsɔOsjdz dʑsfпjsʔ, dzqʙts dзjlsɣqfɔtɕjdзjdʑqf.

ʁ fпgftsdzʟtsɔOʞdzqjʰ qfʷ tɑtsɔOʞdzqfʷ tftɑqf qʜjdʑsqᶠʷqɣOцqfq "ʟOftɑtsfпjtslsɔjls".

ʉ qfdзjdзjlstɑqfɥqfOʸ fпgqfпjsjdзOʰ qfᵂwtɑtsɔOʞdzqfʷ ï ʜtsɣOʟʳ ɔOʸ ʰ qʔ q tgtɑtsɔjtɑʷʁ ʰ qʔ ʜtsdzʞdzʐ qfdзjlsʲ tsвʰ qʔ fпjɣtɕjlsdzʔ ɣdzɥ

ф fпjпgſdzj lstɛſuɋdzΘʸ fпgſfпjsj dzjΟʰ ɋᵂtɛtsɔΘdzɋſʷ ï нtsʕΘLʳ ɔΟʸ ſпɋʔ dzjsʏ j lstʃtɛtsнj dzjtsdzfпjstɛſtɛtsɔΘlsᵘ ɔdzΘнj dzɋſj lsΘʔ dzᵥ dzjʕdzᵥ uɬstdzjtsнdzɋſdzjɋL нɔlzᒐ fпʃtsfпjsʙtsɔ:

– tɛΘfʰj ɋᵂtɛtsɔΘlsᵘ tʃtɛtsuj fпfпj LΟʰ ɋᵂtɛtsɔΘdzɋʔ dzΘjɛtstslsʕtɛʳ lstsdzjʕdzᵥ uj;
– tʃtɛtsfпjsΘɔɋlsᵘ tʃtsн LΘʃtɛtsfпjsdzjfпjtsᵏ uɋᵂtɛtsɔlzᵏ tʃtsнtʃɋfпj.

ɻ tɛɋdzjtɛʳ tʃtɛtslstsʕtsdzɔ ɋнjdls ɋᵂɋʕΟuɋɋ fпʰ ɋᵂtɛtsɔΘdzɋjdzj

1. **tsнdzɔfпjstɛtsdzɔᵂ ɋнjdls ɋᵂɋʕΟuɋᵛ fпɋfпjʃtsdzLtsɔΘdzɋjdzjɔtɛjdzjdzɋ dzjlstsʕ** ï ф ʰ ɋᵂtɛdzjlsdzjlsʕlz ɔtɛjdzjdzɋ ɋ tʃjtɛjнΟʸlsjʸ .I . I , tɛΘfʰj ɋᵂtɛtsɔΘɔ fпjstsʙʰ jdzɋj , tʃtɛtsɔjtɛʷjls, uɬstsɔtɛjdzjdzdzΟʸ dzjlsʕΟ dzΘʔtsнɋlsfпʸ ɔ нtsʃlzfпjsɋdzʏsdzjɋdzdsjtɛɔΘdzj .
2. **tsнdzɔfпjstɛtsdzɔᵂ ɋнjdls ɋᵂɋʕΟuɋᵛ fпɋfпjʃtsdzLtsɔΘdzɋjdzjfпjdzuɋʔ dzᵥ ᒐuɋfпjdzï** .I tʃjtɛjнΟʸlsф LΘʃtɛtsfпj fпjsfпjstsʷʰ ɋʔ ɋL dzj ʕtslststɛtsɋts fпjdzuɋʔ dzᵥɋts uɋfпjdzΟ ф ʰ ɋᵂtɛdzjlsɻlsts uɋfпjdzts ɋ tʃjtɛjнΟʸlsI . ɻ tsdzuɋɔ ɋ tɛΘfʰj ɋᵂtɛtsɔΘɔ fпjstsʙʰ jdzɋj , tʃtsdzLtsɔΘsjdz .I fпjjtɛʷjls tʃtsdzuj dzdzsj uɋfпjdzts fпj tslstʃtɛΘɔdzjdzdzᵥ dzʒ
3. **ɔLΟɋdzjdΟʷ ɋнjdls ɋᵂɋʕΟuɋᵛ fпɋfпjʃtsdzLtsɔΘdzɋjdzjfпjdzuɋʔ dzᵥ ᒐuɋfпjdzï** .I tʃjtɛjнΟʸlsф LΘʃtɛtsfпj fпjsfпjstsʷʰ ɋʔ ɋL dzj ʕtslststɛtsɋts fпjdzuɋʔ dzᵥɋts uɋfпjdzΟ ф ʰ ɋᵂtɛdzjlsɻlsts uɋfпjdzts ɋ dzj ʕtslststɛtsj fпjtsʸ ɋ tʃjtɛjнΟʸlsI . ɻ tsdzuɋɔ ɋ tɛΘfʰj ɋᵂtɛtsɔΘɔ fпjstsʙʰ jdzɋj , tʃtsdzLtsɔΘsjdz .I fпjjtɛʷjls tʃjtɛɔtsj tʃtsdzuj dzdzsj uɋfпjdzts fпjtslstʃtɛΘɔdzjdzdzᵥ dzʒ ɋ, ɔ fпjdzuɋʔ fпjɔtʃΟнjdzɋʷ, tslstʃtɛΘɔdzʸjls ф tslsɔjls, fпjsнjtɛʏΟʰ ɋʔ tsʙΟLΟʰ ɋᵂtɛtsɔΘdzᵥ ᒐuɋfпjdzΟ ɻ Θsjdzʒ ф tɛΘfʰj ɋᵂtɛtsɔʳ ɔΘjls ɋ fпjjtɛʷjls tʃtsdzuj dzdzᵥ j uɋfпjdzΟ uɬsts вʳ dzɋ tslstʃtɛΘɔdzjdzᵥ .

ɸlsΟʕɋ dΟtʃtɛtslstsʕtsdzᵥ ɋнjdls ɋᵂɋʕΟuɋɋ ɋ dzjlstsнʳ LΟʰ ɋlsʳ

1) <u>tʃtsнdzjdzΟ</u>ï tʃtstʃʳ lsʕΟtʃtsнdzjdzɋlsᵘ tsнdzsɋts tʃtsdzLtsɔΘsjdzʸ нtɛzɋʔdzʒ ***ʃ j lstsнʳ tʃtɛtslsɋətsnj ʔ fпjs əɋʷ*** fпjsfпjstsʷls ɔ fпjsᒐtɛΘdzjdzɋɋ ɔ lsΘʔ dzj tslstʃtɛtslsɋəɋʕΟɋɋʷ tstɛɋʒΟuɋɋ, tstʃtɛjнjdzʷʁ ʰ j ʔ Θdzɋtstɛɋlsdzʒ ɋнjdzɋsɋʷ ɋʕΟuɋɋ.
2) <u>tʃtɔlststɛdzɋsj dzΘɔʷLʳ ɔΘdzɋj fпjstsʙʰ jdzɋʷ</u> ï tʃtsнdzjdzΟɋɋ нtɛzɋtsʔ dzjlstsн tsʙdʒΘdzΟ ɋfпjʃtsdzLtsjdzʒtsʔ ɋɋʷ tstɛɋʒΟuɋjʔ tɛΘdzjj tʃtɛtsɔj нʸ dzdzsɋts tʃtɛtslstsʕtsdzΟɋnjdzɋsɋʷ ɋʕΟuɋɋ lstsɋts xj fпjΘdʒtsɋts ɋdzɋ нtɛzɋtsɋts tʃtsdzLtsɔΘsjdzᵥ. ***ʃ j tɛʳ tʃtɛtslsɋətsnj ʔ fпjs əɋʷ*** ɔʕdzᵥ uΟʰ lsɋfпjʃtsdzLtsɔΘdzɋjtʃtɛtslstsʕtsdzɔ lsɋtʃΟ"LΟʃtɛtsfпjtslsɔjls", ɋfпjʃtsdzLtsɔΘdzɋj ɔtɛjdzjdzdzᵥ ᒐdzjlstsʕ, fпjdzuɋʔ dzᵥ ᒐuɋfпjjdzɋɋdzɋ ɔtsLtɛΘfпjsΟʰ ɋᵂ tʃtsfпjdzнtsɔΘsjdzdzsfпjsjʔ uɋfпjjdz
3) <u>ʕtsdʒɒɋdzɋtɛtsɔΘdzdzᵥ j ΘsΘʕɋ</u>ï tʃtsнdzjdzΟɋɋ нtɛzɋtsʔ dzjlstsн tsʙdʒΘdzΟ ɋfпjʃtsdzLtsɔΘdzɋj ʕtsdʒɒɋdzΟuɋʔ нΘdzdzᵥ ᒐɋL tɛΘdzjj ɔʳ tʃtsdzdzjdzdzᵥ ᒐtʃtɛtslstsʕtsdzɔ, ɔ lstsdzɋuɋfпjdzj tʃtɛtslstsʕtsdzɔ, tɛΘdzjj dzΘɔʷLΘdzdzᵥ ᒐtʃtɛtslsɋədzɋʕtsdzʒ ***ʃ j lstsнʳ tʃtɛtslsɋətsnj ʔ fпjs əɋʷ*** fпjsfпjstsɋls ɔ tsʙj fпjj uj dzɋɋ uj dzsfпjsdzsfпjsɋ tʃtɛtsɔtsнɋdzʒ ᒐtʃtɛtslstsʕtsdzɔ ɋtslsнj dzdzᵥ ᒐfпjstsʙʰ jdzɋʔ .
4) <u>ΘsΘʕΟtslstɛΘjdzɋjdzʒ</u>ï ʕtsdʒɒɋdzɋtɛtsɔΘdzdzΟʸ ΘsΘʕΟɋ ɋfпjʃtsdzLtsʷ tʃtsfпj dzʕlz uΟfпjsɋ tʃtɛɋdzʷlstsʔ ɋdzʷ tstɛɋʒΟuɋɋ нtsʕΟLʳ ɔΟʰ jdzʒz. ***ʃ j lstsнʳ tʃtɛtslsɋətsnj ʔ fпjs əɋʷ*** ɔʕdzᵥ uΟʰ ls ɔɔjнjdzɋjɔ tʃtɛtslstsʕtsdzɋнjdzɋsɋʷ ɋʕΟuɋɋ tstɛɋʒΟuɋɋ tʃtɛtsɔjtɛʷʁ ʰ jɋts, ɋfпjʃtsdzLtsɔΘdzɋj tɛΘdzɋuɋʔ нdzʸ tʃtɛɋʸdzʒΟɋ tʃjtɛjнΟuɋ fпjstsʙʰ jdzɋʔ .
5) <u>LΟнjtɛʏʕΟtʃjtɛjнΟuɋ fпjstsʙʰ jdzɋʷ</u> ï tʃjtɛjᒐɔΘs tʃtɛtslsɋədzɋʕtsdzʒ fпjstsʙʰ jdzɋʷ ɋ dzΘɔʷLʳ ɔΘdzɋj jɋts ɔ вtsdzjj tʃtsLнdzɋʔ dzʒsdzjdzls ɔtɛjdzjdzɋ. ***ʃ j lstsнʳ tʃtɛtslsɋətsnj ʔ fпjs əɋʷ*** ɔʕdzᵥ uΟʰ ls ɋfпjʃtsdzLtsɔΘdzɋj fпjdzuɋʔ dzᵥ ᒐuɋfпjjdzfпjsɔdzjfпjsdzts fпjsɋtɛΘdzɋjuj dzɋj dzʒ ɔtɛjdzjdzdzsɋts tʃtɛtsdzjxjzlsʕΟнdzʸ tslsɔjlsΘ) ɋfпjʃtsdzLtsɔΘdzɋj ɔtɛjdzjdzdzᵥ ᒐdzjlstsʕ.
6) <u>ɋfпjʃtsdzLtsɔΘdzɋj tʃtɛtslsɋədzɋʕtsdzʒ fпjtsɋᒐ fпjsjнfпjsɔ ɔ ʕΟujfпjsɔj uΟfпjsɋ lsjdzʕtsdzʒdzdzɋʕΟuɋtsdzdzsʔ fпjstɛdzʕlsdzɛʳ</u> ï ΘsΘʕΟ tʃtɋ ʕtslststɛtsʔ dzjxнlzф ɋ .I tʃtɛtslsɋədzɋʕ ʉ ɔᒐtsнɋlsɔ lsjdzʕtsdzʒdzdzɋʕΟuɋtsdzdzᵥ ʔ ʕΟdzΘdzɋ fпjsΘdzsɔɋlsfпʸ jɋts uΟfпjsʳʁ . ɻ tɛɋʲlstsdzʒtʃtɛtslsɋədzɋʕ dzjsxjls tʃtsнdzjdzɋlsᵘ ɋdzʷ tstɛɋʒΟuɋʁ , tʃjtɛjнΟɔΟjdzʸᶻ dzjxнlzф ɋ .I . ***ʃ j lstsнʳ tʃtɛtslsɋətsnj ʔ fпjs əɋʷ*** ʲlstsʔ ΘsΘʕj fпjsfпjstsɋls ɔ ɋfпjʃtsdzLtsɔΘdzɋʃɋ lΟʰ ɋʰ ʸ dzdzsɋts ʕΟdzΘdzΟdzjxнlzф ɋ .I .

IV. Криптосистемы с открытым ключом

Криптосистема RSA (названа по первым буквам фамилий авторов Rivest, Shamir, Adleman) – первая криптосистема с открытым ключом, которая оказалась пригодной и для шифрования, и для цифровой подписи. Ее стойкость основана на сложности факторизации больших целых чисел.

Криптосистема Рабина – криптосистема с открытым ключом, стойкость которой эквивалентна сложности факторизации. Недостатком криптосистемы является то, что каждому зашифрованному сообщению соответствуют четыре равновероятных открытых сообщения, поэтому однозначное расшифрование невозможно.

Криптосистема Эль-Гамаля – криптосистема с открытым ключом, основанная на сложности вычисления дискретных логарифмов в конечном поле. Криптосистема Эль-Гамаля используется в стандарте цифровой подписи США.

IV.1. Криптосистема RSA

Генерация ключей

- Выбираются два различных случайных простых числа p и q заданного размера (например, 1024 бита каждое).
- Вычисляется их произведение n = p·q, которое называется модулем.
- Вычисляется значение функции Эйлера от числа n: φ(n) = (p − 1)(q − 1).
- Выбирается целое число e, 1 < e < φ(n), взаимно простое со значением функции Эйлера φ(n).
- Вычисляется число d, мультипликативно обратное к числу e по модулю φ(n), то есть такое, что e·d ≡ 1 (mod φ(n)).

Шифрование

- Сообщение разбивается на блоки, каждый блок представляется в виде целого числа m, 0 ≤ m < n.
- Вычисляется шифротекст c = m^e mod n.

Расшифрование

- Вычисляется m = c^d mod n.

Пример

1. Выберем простые числа p = 11, q = 13.
2. Вычислим n = 11·13 = 143.
3. Вычислим φ(n) = (11 − 1)(13 − 1) = 120.
4. Выберем e = 7.
5. Вычислим d = 103, так как 7·103 = 721 = 6·120 + 1.
6. Открытый ключ: (e, n) = (7, 143).
7. Закрытый ключ: (d, n) = (103, 143).
8. Зашифруем сообщение m = 9: c = 9^7 mod 143 = 48.
9. Расшифруем: m = 48^103 mod 143 = 9.

Атаки на RSA

- Если злоумышленник может факторизовать n, он может вычислить φ(n) и затем d, поэтому стойкость RSA основана на сложности факторизации.
- Если e и d малы, то d можно найти перебором.
- Если m мало, то m^e < n, и c = m^e, поэтому m можно найти как обычный корень степени e.
- Если два пользователя имеют общий модуль n, то они могут расшифровать сообщения друг друга.

Теорема Рабина

Пусть n = p·q, где p и q – различные простые числа, и пусть c – квадратичный вычет по модулю n. Тогда сравнение x^2 ≡ c (mod n) имеет ровно четыре решения.

Доказательство

1. Сравнение x^2 ≡ c (mod p) имеет ровно два решения, так как c – квадратичный вычет по простому модулю.
2. Сравнение x^2 ≡ c (mod q) имеет ровно два решения, так как c – квадратичный вычет по простому модулю.
3. Пусть x_1 – решение сравнения x^2 ≡ c (mod p), а x_2 – решение сравнения x^2 ≡ c (mod q).
4. Тогда существуют ровно четыре решения сравнения x^2 ≡ c (mod n), которые можно найти с помощью китайской теоремы об остатках.

Вычисление квадратного корня по простому модулю

Пусть p – простое число вида p = 4k + 3, и пусть c – квадратичный вычет по модулю p. Тогда $x = c^{(p+1)/4} \bmod p$ является решением сравнения x^2 ≡ c (mod p).

Доказательство

1. Так как c – квадратичный вычет, то $c^{(p-1)/2} \equiv 1 \pmod p$.
2. Возведем обе части в квадрат: $x^2 = c^{(p+1)/2} = c \cdot c^{(p-1)/2} \equiv c \pmod p$.

Пример

1. Пусть p = 11, c = 3.
2. Вычислим x = 3^3 mod 11 = 27 mod 11 = 5.
3. Проверим: 5^2 = 25 ≡ 3 (mod 11).
4. Решения сравнения x^2 ≡ 3 (mod 11): x = 5 и x = 6.

Китайская теорема об остатках

Пусть m_1, m_2, …, m_k – попарно взаимно простые натуральные числа, и пусть a_1, a_2, …, a_k – произвольные целые числа. Тогда система сравнений x ≡ a_i (mod m_i), i = 1, …, k, имеет единственное решение по модулю M = m_1·m_2·…·m_k.

Доказательство

1. Для каждого i положим M_i = M / m_i.
2. Так как m_i и M_i взаимно просты, существует обратный элемент y_i такой, что M_i·y_i ≡ 1 (mod m_i).
3. Положим x = a_1·M_1·y_1 + a_2·M_2·y_2 + … + a_k·M_k·y_k.
4. Тогда x ≡ a_i (mod m_i) для каждого i.
5. Если x' – другое решение, то x − x' ≡ 0 (mod m_i) для каждого i, поэтому x − x' ≡ 0 (mod M).

Пример

1. Пусть m_1 = 3, m_2 = 5, m_3 = 7, a_1 = 2, a_2 = 3, a_3 = 2.
2. Тогда M = 3·5·7 = 105.
3. M_1 = 35, y_1 = 2, так как 35·2 = 70 ≡ 1 (mod 3).
4. M_2 = 21, y_2 = 1, так как 21·1 = 21 ≡ 1 (mod 5).
5. M_3 = 15, y_3 = 1, так как 15·1 = 15 ≡ 1 (mod 7).
6. x = 2·35·2 + 3·21·1 + 2·15·1 = 140 + 63 + 30 = 233 ≡ 23 (mod 105).
7. Проверка: 23 mod 3 = 2, 23 mod 5 = 3, 23 mod 7 = 2.

Алгоритм Тонелли – Шенкса

Алгоритм Тонелли – Шенкса вычисляет квадратный корень по простому модулю p, если p = 4k + 3.

1. Вычислить k = (p − 1)/4.
2. Вычислить x = c^(k+1) mod p.
3. Вернуть x.

Пример

1. Пусть p = 11, c = 3.
2. k = (11 − 1)/4 = 2.
3. x = 3^3 mod 11 = 5.
4. Вернуть 5.

Алгоритм Рабина – Миллера

Алгоритм Рабина – Миллера проверяет, является ли число n простым.

1. Выбрать случайное число a, 1 < a < n − 1.
2. Вычислить r = a^(n−1) mod n.
3. Если r ≠ 1, то n составное.
4. Иначе повторить шаги 1–3 несколько раз.
5. Если n прошло все проверки, то n, вероятно, простое.

4. Or ucfhqkzcls $t = r * \prod_{i=1}^{m} a_i^{S_i} mod\ n$
5. tfts HtfcfhjsF HdW fhjstsBh j,dkcfw M tftsdksxlcls tfOkdz (s, A)

Fdkstscfls dztftstsej tcSfcf^1

1. tfts tslsSctcr lstscdzlzSdz ucz $b_1, b_2, \ldots, b_m$ mod n cf LdkOujdkcfg t Or ucfhqkzcls :
   $w = t^2 * \prod_{i=1}^{m} b_i^{S_i} * mod\ n$
2. Or ucfhqkzcls n(M, w) = S/
3. tftstsej,tccfls tcOej,dkfhsotsS = S/

1 tccfdzj tcSfcfdzjSfhqtsz? fhqfhjsj,dz tstcOkdcfLOucfcf dOHy xldtsfhjscf fgwLcf

1) lzfhjsOktsodzjdkcfj fgwLcf;
2) Ozlsj,dksfw cfSOucfw fhjststsdtsdzfhjcfj,dzj tcOucfj? fhjOkdfhjsotsgtsSdz uO
3) tstcgOkdcfLOucfw fgwLcf fhjststsdtsdzfhjx1 tfj,tcej,HOeOgj,dz? Cr HOkdzk Cr Sdz ucfsdz (cgj,dzj tccftstsoOkdcfj,dkO 1 lsOfj,Ozlsj,dksfw cfSOucfcf);
4) tfj,tcej,HOeOgj,dz? j,fhjstsBh j,dkcfw HtsftfsdzdzwBg lsfhy fgy tdlsSts? (HdW Htsoj,tcwBg h cfCr fhjststsdtsdzj cfdzcf x1 (HdW dzj,Htsoj,tcwBg h cfCr fhjststsdtsdzj cfdzcf HtsSlzdzj,dksts HdW tsBj,fhjfj,ujdkcfw ujdksfhjsdksfhjscf, Oo fhqkzucgj x1 ï j,h y cf dzj,fhjftsfhjsBdksfhjscf, tfj,tcej,HOeOgj,dzs? cfdkw tstcdzjOucfcf;
5) oOldkOy cfdkw tstcdzjOucfw Htsdxldkoh cfw tdtsoOls fhy tfj,tcej,H tslstftcOeSts?, HOlj,dzj,fhqkzslstcw dkO h cfw tdtsoOkdcfj,o SOkdkOdzj fgwLcf. z, cfw tcdzj,lsfhy cfdkw tstcdzjOucfw odzjfhjsj,fhjftsHtfcfhjBg cfdzcf fgy tdlsSts?.
6) ots otej,dzw fhjOkdfhjOfgwLcf otsLdkzsxldz tftdtsujHzdcr tftso lststcdkds? Ozlsj,dksfw cfSOucfcf.

IV.2. R dkw tstcdzjOucftsdkdkOy Bj,LtstfOfhqtsfhjs1 (R 1)

1 tsdkflscfSOR 1

R dkw tstcdzjOucftsdkdkOy Bj,LtstfOfhqtsfhjs1 ï x1 lsts Sdtsdzfdzj,Sfhjdzjtc, tsBj,fhjfj,ucfoOy h cf? HdW tsCoOlr oOj,dzks? cfdzj cfdkw tstcdzjOucfcf fhqkz,Hlzg h j,j,:

- **Sdtsdkw cfHj,dkucfOdkdtsfhjs1** ï otsLdzksxldtsfhjsh tsLdkOSdtsdzjdkcfw fhjcfdkw tstcdzjOucfj,? cfdzjg ls o fgdtsy dzj tcOfhjfstcwxlj,dkcfcf lstsdzSdts lsj dkcfucO,Sdts odkOujj,ls fhjstslsoj,lsfhjsolzg h cfdzjcf tfjtsdkdtsdzjsucfwdzjcf;
- **ujdksfhjsdtsfhjs1** ï otsLdzksxldtsfhjsh odzjfhjscf cfLdzjdzjdkcfw o cfdkw tstcdzjOucfg Htsdxldz cfdzjls lstsdzSdts lsj dkcfucO,Sdts dkOx1 lsts lzfjtsdkdtsdzjsujdz,
- **Htsfhjslzfdtsfhjs1** ï otsLdzksxldtsfhjsh tfjtsdkzujdkcfw Oolststcfjtsoldkdtsgcts Htsfhjslzfjtsdkw tstcdzjOucfcf fhjs fhjststsdtsdz tfjtsdzLtsoOlsj,dzw o fhjstslsoj,lsfhjsolzg h cf?, fhqkzSucfjtsdkdcfjtsoOkdkdz? Hdw tcOotslsr, tfj,tcfjtsH otej,dzj,dkcf;
- lzucy ls ï ofhjLdkOucfdzj,Hj,?fhjsocfw tfjtsdzLtsoOlsj,dzj,? (HOlj,j,fhqkzcfjtsdkcfdzj,or CrtsHwlsLOtcOkfSdcf, tsfjtej,Hj,dzdkdtsgcts Hdw x1 lstsgcts tfjtsdzLtsoOlsj,dzw tfjtcOocfdz), Htsdxldz Br ls LGwcfSfhqjtstsoOkdz cf tfjtcsOkdkdzjLcfjtsoOkdz ;
- dzjtslstej,SOj,dzjsfhjsh cfdkcf Ofj,dzkdzjtcdzj,dzjsfhjsh ï tfjtsdzLtsoOlsj,dz, dkOjtcOocfoh cf? cfdkw tstcdzjOucfcy Htcdzgctsdzjdz tfjtsdzLtsoOlsj,dz , dzj,dzjsxlj,ls tslstej,ucf fhy tsls w OSlsOdkOjtcOodzj,dkcfw cfdkw tstcdzjOucfcf, O tfjtsdzLtsoOlsj,dz , tfjtsdzucfoh cf? cfdkw tstcdzjOucfcy , dzj,dzjsxlj,ls tslstej,ucf fhy tsls w OSlsOj,y tfjtsdzucj,dkcfw.

1 tsdkflscfSOR 1 ï x1 lsts dkOBtstcw tstcdzjOdzdz. C (tsw cfucfOdz dzs lzlsoj,tcxlHy dkdz. C dzfBts lstcOHcfucfjtsdkdkdzs fhqkzsxlcfoh cfCrfhy) tftcOocfdz,Sfslststcr j,tcej,gdkOdzj,dkdsftcdzgy ls w lzdkSucfjtsdkftstcOokfj,dzj,CrOokfLdzOcfdkw tstcdzjOucfjtsdkdkdzs? Bj,LtstfOfhqtsfhjscf.

f,j,COkdfLdzy R 1

- cfHj,dkdsfw cfSOucfw ï tstftcej,Hj,dzdkdz? (tcOfhjftsLdkOOokfj,) SOlHr? lzuOfhjstsS tftdtsujfhjfO cfdkw tstcdzjOucfjtsdkdkdzs olLOtfdzjsHj,?fhjsolzj,lsftj,tcej,H lsj,dz,SOS Sdj,dzjz B lzHlzls tftcfdzj,dj,dz SOScfj,-dzfBts tftsdzwlsfw cfdkw tstcdzjOucfjtsdkdkdzs? Bj,LtstfOfhqtsfhjscf.
- Ozlsj,dksfw cfSOucfw ï tftsHlsoj,tcxlHj,dkcfj, cfHj,dksfw cfSOucfcf;
- Sdtsdkstdtsdz HtsfhjslzfjtsfOï fhjsLHOkdkcfj, cf tftsHHj,tcxlOkdkcfj, dkOBtstcOtftcOocfdz,tstftcej,Hj,dzdkdz j,SOlHtsdzjz lzuOfhjsdkcfSlz tftdtsujfhjfOcfdkw tstcdzjOucftsdkdkdzsgcts tsBdzj,dkOtcOLtcej,h j,dkcfj, dkOHtsfhjslzfjtej,fhjtcfhjOtzcf lzdtsodz x1 lstsgcts HtsfhjslzfjtsfO
- Oolststcfjtsfucfw ï ww tstcdzjftdtsowcfdzw tftcOo HdW Sdtsdkstdtsdzw Sdtsdkftej,lsdksgcts lzuOfhjsSfO tftdtsujfhjfOcfdkw tstcdzjOucftsdkdkdzsgcts tsBdzj,dkO(Ozlsj,dkw cfucftdtsoOkdkdzsgcts cfdzcf Okdksdkcfdzjksgcts) cfL dkOBtstcOtftcOocfdzSdtsdkstdtsdzw HtsfhjslzfjtsfO)

- ⁄ÐzнcƒlsÇ cÑ dдysdжƒlstsтaÇdжc¨ï tдjсdzÐwtaÐdтsj tslsfпdjэ xÇ qэ⁄Ðdжƒj fптsвr lsÇ?, tƒtдtsÇfпF tsнwfh qÑ⊐ э tƒtдtsчjfпfпj tsвdэjdж⁄ÇqÐdжwtstaÐэ⁄uÇqj?, fптдjсÇqfпhstа⁄uÇqj? qÇ⁄Ðdж⁄ÐdжƒLtsdэtƒtдjнtsƒtдjнj dzÐdжz⊐, LdжF⁄uÇqÐdэ⁄ ⊐cÐdжƒ tƒtsнtsLtaÇqlsjdzÐdz⊐fптsвr lsÇ?.

ф lzнcƒlsÇtƒtдjнtƒtsdж⁄⁄G⁄jls⁄Ðdж⁄ÐdжƒL fптsвr lsÇ? tƒtsfпhsw⁄G¶lslzdэ⁄⁄ÐdэtsdжƒlstsтaÇdж¨ï tƒtaÇqвdжƒxjjÐdжs¶tдjxÇqÐdэhz tдj⁄Ðdzdжstsсtsэtдjdэjdж.

- tдj⁄Ð⁄ÇqÐtaтsэ⁄Ðdжƒj dж⁄Ðcqdжuqcнjdжs ï fптsэts¶lzƒdжsfпhsu tƒtдtsчjнlzтc¨cÇ dэjtдtsƒtaÇqwlsÇ?, ¶tslststc¨ j tƒtдtsqLэtsнwlsfпy tƒtaÇ dж⁄Ðdzh j dжƒqÇ cÑdжƒ tƒtsнtsLtдjdжƒqÇ dж⁄Ðdж⁄Ðdzh j dжƒj cÑdжwtstaÐэ⁄uÇqtsdжdжs? вj LtstƒÐfпhsdжsfпhsqÇ.
- lzƒtа⁄эdдjdжƒj ¶tsdzw cÑdzтa⁄Ouqj? ï fптsLнÐdжƒj cÑ tƒtsннj tа¬xÐdжƒj w lzdж¶uÇqtsdжƒtдtsэ⁄Ðdжƒqwfптдjнr cÑdжwtstaÐэ⁄uÇqtsdжdжs⁄ts tsвdэjdж⁄эtsdжdжs⁄ts tsвdэjdж⁄Ðэ tа⁄эbtslstsfпjtsfптsвdжsdэfптshstswdжƒqÇ cÑэ fптstslsэj lsfпhsэcÑ fпlstдjвtsэ⁄Ðdжƒwdэ[R ɹ;
- lzƒtа⁄эdдjdжƒj tƒtsdzLtsэ⁄Ðsjdzwdэ[ï tsвj fпƒj ujdжƒj lzfпdжsэ?tа⁄эbtslsr tƒtsdzLtsэ⁄Ðsjdzwэ fптдjнj cÑdжwtstaÐэ⁄uÇqtsdжdжs⁄ts tsвdэjdж⁄Ðэ fптstslsэj lsfпhsэcÑ fпlstдjвtsэ⁄Ðdжƒwdэ[R ɹ;
- lzƒtа⁄эdдjdжƒj tдcƒfпF⁄Ðdэ[ï tsвj fпƒj ujdжƒj fптstslsэj lsfпhsэcÑw эtsLdэtsxÇdz⊐tƒtslsjtдr tslsdж⁄Ðdzh j dжƒw R ɹ cÑdэtsh dжsfпhsqÇ L⁄Ðy cÑlsdz⊐fптдjнfпhsэ;
- tsвj fпƒj ujdжƒj lzfпhsts? uÇqэtsfпhsqÇ ï tƒtsннj tа¬xÐdжƒj fптдjнr cÑdжwtstaÐэ⁄uÇqtsdжdжs⁄ts tsвdэjdж⁄Ðэ dэ[dжƒqdэ[⁄Ðdzdжs нtsƒlzfпhsqÇdэtsdэ[tа⁄эbtslstsfпjtsfптsвdжsdэfптshstswdжƒqÇ cÑ fптstslsэj lsfпhsэcÑj lstдjвtsэ⁄Ðdжƒwdэ[R ɹ э lzfпdжsэcÑw⊐нj fпhstdz¶lsÇэdz⊐fптдjнfпhsэ?fпhsэcÑ?.

∫ fпdжsэdz j cÑdfпhstdzdjdжs r R ɹ

- tƒj tаfптsdж⁄Ðdz ï dz нcÑ, ¶tslststc¨ j вlzнlzls tsвj fпƒj ujcÑэ⁄Ðs tƒtдjls tsвtдjsэtsdjdжƒj э xÇ qLdz R ɹ;
- dжstadэ⁄Ðsqэdжsj tsвj fпƒj ujdжƒj ï нts¶lzdэjdжs r, ¶tslststc¨ j fптsLнÐ ls tƒtа⁄эbtsэtsj tƒtдtsfпhsta⁄Ðdжfпhsэts нdz w lzdж¶uÇqtsdжƒtдtsэ⁄Ðdжƒw R ɹ;
- dэtsнjdэdж⁄Ðy вj LtstƒÐfпhsdжsfпhsu ï fпF¬jdz r tsвj fпƒj ujdжƒw R ɹ, L⁄Ðdжsxjdжdz j э н⁄Ðdжdжz g ¶tsdж¶tдjlsdжz g cÑdжwtstaÐэ⁄uÇqtsdжdжz g fпƒfпhsjdэz cÑdжƒ fптдjнlz;
- ¶tаcƒtƒlstsc¨ta⁄Ðw cÑw;
- ⁄Ðdжsqэcƒtа⁄zfпdжsj tsвj fпƒj ujdжƒj;
- dэjxÇ fпjlsjэr j ɹ¶tа⁄Ðdz ï w ⁄Ð?jtаэtsdz;
- fпF⁄Ðdж⁄tc¨ вj LtstƒÐfпhsdжsfпhsqÇ ï lzfпhstдts?fпhsэ⁄Otƒtдtsэjta¶cÇ ¶⁄Ðuj fпhsэ⁄Ow lzdж¶uÇqtsdжƒtдtsэ⁄Ðdжƒw cÑdжwtstaÐэ⁄uÇqtsdжdжs? dэtsнjdzƒвj LtstƒÐfпhsdжsfпhsqÇ нdz нtsdэ⁄);
- fпƒfпhsjdэ⁄tsвdж⁄Ðdz xjdжƒw ⁄Ðs⁄¶ï lzfпhstдts?fпhsэ⁄OdэtsdжƒlstsтaÇdж¨⁄Ð¶lsÇэdжsfпhsqÇ э cÑdжwtstaÐэ⁄uÇqtsdжdжs? fптдjнj, cÑdжsc¶н⁄OfпэtsLdэtsxÇdжsfпhs u ƒtдtaÇdzwlsÇw fпy⁄dэtsfпhstswlsjdzdжsc¶ts lzu⁄fпhsqÇw э lz¶⁄O⁄Ðdжdжs? ⁄¶lsÇэdжs? нjw lsjdzdжsfпhsqÇ
- tдjLjtаэdжsj ¶tsƒtдcƒtдtsэ⁄Ðdж⁄jj;
- нlzвdжƒtдtsэ⁄Ðdжƒj;
- ⁄э⁄Ðdжaq?dz?ƒtдdж⁄Ðdzï dж⁄эbtstc¨dэjtдtsƒtдaÇwlsÇ?, tƒtдtsэtsнcÑdэ⁄ ⊐ƒtдaÇ dж⁄Ðdzh j dжƒqÇ tƒtдa⁄эbcÑdzR ɹ;
- tsвlzujdжƒj tƒtsdzLtsэ⁄Ðsjdj?ï tsвlzujdжƒj tƒtsdzLtsэ⁄Ðsjdj?ƒtдa⁄эbcÑdж⁄Ðdэ⁄tа⁄эbtslsr э fптstslsэj lsfпhsэcÑ fпlstдjвtsэ⁄Ðdжƒwdэ[R ɹ.

∫ fпdжsэdz j dж⁄Ðƒtа⁄эdдjdжƒw R ɹ

1. **w cÑLcÑujfпF⁄Ov вj LtstƒÐfпhsdжsfпhsu** ï tsвj fпƒj ujdжƒj fптs⊐tа⁄Ðdжƒw tsвtstdzнtsэ⁄Ðdж⁄w, tƒtдjнdж⁄Ldж⁄ujdжdжs⁄ts нdz w lzdж¶uÇqtsdжƒtдtsэ⁄Ðdж⁄w cÑdжwtstaÐэ⁄uÇqtsdжdжs? fптдjнr, ¶tsdжstдtsdz нtsfпhslzƒ⁄Odz нj? ¶ɹlstsdэz tsвtstdzнtsэ⁄Ðdж⁄g, L⁄Ðy cÑls⁄ƒtsdzLtsэ⁄Ðsjdj? cÑdжwtstaÐэ⁄uÇqtsdжdжs? fптдjнr tsls w cÑLcÑujfпF¬tsc¶ts эtsLнj? fпhsэcÑw Ldжslzdэr h djdжdжaq¶⁄O⁄Ols⁄xjjL⁄Oy cÑlsr cÑdжwtstaÐэ⁄uÇqtsdжdжs? djэcÑtdslzÐdz dжsc¶ts ⊐⁄Ða⁄¶lsjta⁄O(ta⁄fпƒjujÐsts¶, fпdzxjвdz⊐lsjdjw tsdжsэé).
2. **¶tsdэƒr ls j tdzO⁄v вj LtstƒÐfпhsdжsfпhsu** (fпjlsjэ⁄Oy вj LtstƒÐfпhsdжsfпhsu, lsjdj¶tsdэ⁄zdжa¶⁄uÇqtsdжdж⁄Oy вj LtstƒÐfпhsdжsfпhsu, вj LtstƒÐfпhsdжsfпhsu нÐdжdz⊐) ï tsвj fпƒj ujdжƒj L⁄Oy cÑlsr cÑdжwtstaÐэ⁄uÇqcÑэ j y эcÑtdslzÐdz dжsdэ⁄эcÑнj.
3. **вj LtstƒÐfпhsdжsfпhsu нÐdжdz⊐** ï tsвj fпƒj ujdжƒj L⁄Oy cÑlsr cÑdжwtstaÐэ⁄uÇqcÑэ j y эcÑtdslzÐdz dжsdэ⁄эcÑнj.

¶ taÇlsjtaÇcÑdj¶tsв⊐tsнcÑdэtsfпhsc Ñ fпtsLнÐdжƒw fпdzxj вr R ɹ

- dж⁄Ðdжƒ⁄uÇqj э w qtaÐэjвtsdz h j 10 ¶tsdэƒu lsjtдtsэ, ta⁄Ofпƒtдjнj dz dжdz⊐ tƒts tƒtsdэjfh j dжƒw dэ;
- dж⁄Ðdжƒ⁄uÇqj э w qtaÐэj dжs¶⁄Ðdz dжs? fпjlsÇ;
- dж⁄Ðdжƒ⁄uÇqj tƒtsн¶dz ujdжƒw fпjlsÇ w qtaÐэ ¶ cÑdжsjtaÐj⁄lsz;

- dҿ·dҿɽʃɥɖʝ dʒsʜʝdʒʘ·ᴞtslsʷ ʙʳ dҿʘtsʜdҿsdʒɖʟ ʢtsdʒʄᴵᴮ lsʝtҽtsɘ ʬɖtҽdʒʳ (dҿlzɥlsʸ dҿdҿsʝ tʃtsʜʢdҿ ɥʝdҿʃʝ ʢ fiʝ lsɖ);
- dҿʘdҿɽʃɥɖʝ ᴞtslsʷ ʙʳ dҿʘtsʜdҿsdʒ ʢtsdʒʄᴵᴮ lsʝtҽʝ ɖdҿʬ tstҽdʒʘ·ɥɖɖ, tҽʘ·ʟɢdҿʘ ʝdҿʃʝ ɖdҿɽʃ lzlsʝtҽʷ ʢtslststҽtsʡ dʒsʞʝ ls tʃtҽɖdҿfiʝsɖ ʬɖtҽdʒʝ filzʰ ʝ fiʝsɘʝdҿdҿ ʡ lzʰ ʝtҽʙ.

ʇ tsdҿʃls ɖʢʘʀ ᴊ

- tstҽɢʘ·dҿʃʟʘ·ɥɖtsdҿdҿ ʝ dʒʝtҽʳ ï tʃtҽʘ·ɖdҿʘtʃtsɘʝʜʝdҿʃʷ tʃtsdҿʟtsɘʘ·lsʝdҿʷ, ʘʜdʒɖdҿʃfiʝtҽʘ·lststҽtsɘ ɖ fiʝlstҽlzʜdҿʃʢtsɘ fiʝdҿʞʙʳ ʀ ᴊ, ɖᴞ tʃtҽʘ·ɘʘ·ɖ tsʙʷʟʘ·dҿdҿsfiʝsɖ;
- ʘʄtʃʘ·tҽʘ·lsdҿ ʝ ɖ tʃtҽtsɢtҽʘ·dʒdʒdҿ ʝ fiʝtҽʝʜfiʝsɘʘ·ï ʢtsdʒʄdҿʢfiʝʬɖʟɖɥʝfiʢɖᴞ ɖ ɘɖtҽlslzʘ·dҿdҿ ᴞ fiʝtҽʝʜfiʝsɘ, tʃtҽʝʜdҿʘ·ʟdҿʘ·ɥʝdҿdҿ ᴞ ʜdҿʸ tҽʝ ʘ·dҿʃʟʘ·ɥɖɖ tʃtҽʘ·ɘ ɖ tsʙʷʟʘ·dҿdҿsfiʝsʝ ʡ tʃtsdҿʟtsɘʘ·lsʝdҿʡ, ʘʜdʒɖdҿʃfiʝtҽʘ·lststҽtsɘ ɖ fiʝlstҽlzʜdҿʃʢtsɘ fiʝdҿʞʙʳ ʀ ᴊ.

ʇ tҽtsɢtҽʘ·dʒdʒdҿs-ʘʄtʃʘ·tҽʘ·ls dҿ ʝ fiʝtҽʝ ʜfiʝsɘʘ

- ʘʄtʃʘ·tҽʘ·lsdҿs-dҿʟʘ·ɘɖfiʝɖdʒʳ ʝ ï tҽʘ·ʙtslsʘʰ ɖʝ ʙʝʟ lzɥʘ·fiʝsɖʷ ʘʄtʃʘ·tҽʘ·lsdҿ ᴞ fiʝtҽʝʜfiʝsɘ ʟʘ ɖlsʳ ɖdҿʬ tstҽdʒʘ·ɥɖɖ ï tʃʘ·tҽtsdҿ, tʃtҽtsɢtҽʘ·dʒdʒʳ ʰ ɖʬtҽtsɘʘ·dҿʃʷ, ʘ·dҿlsɖɘɖtҽlzfiʝ ;
- ʘʄtʃʘ·tҽʘ·lsdҿs-ʟʘ·ɘɖfiʝɖdʒʳ ʝ ï tsʙʝfiʝʝɥʝdҿʃʝ fiʝstʃtҽʷʞʸdҿdҿ ᴞ ʘʄtʃʘ·tҽʘ·lsdҿ ᴞ fiʝtҽʝʜfiʝsɘ ʟʘ ɖlsʳ ɖdҿʬ tstҽdʒʘ·ɥɖɖ fiʝʜtҽlzɢɖᴞ tʃtҽtsɢtҽʘ·dʒdʒɖdҿʃ ʃ ʉ ï ʜtҽʘʡɘʝtҽʘ fiʝtsʙtsʜdҿsʝ ʇ ʃ ;
- ʘ·ɘlstsdҿsdʒdҿ ʝ ï ɥʘ·fiʝsᴵ fiʝʃfiʝsʝdʒʟʘ ɖlsʳ ʬlzdҿʢɥɖtsdҿʃtҽlzʝ ls fiʝʘdʒsfiʝstsʷlsʝdҿ dҿs ï fiʝʃfiʝsʝdʒʳ ɘɖʜʝtsdҿʘ·ʙdҿ ʜʝdҿʃʷ, ʜtsdʒsʬtsdҿdҿʘɘᴞtsʜʝ ɘ tsʬɖfiʝ
- ʢtsdʒʄdҿʢfiʝdҿ ʝ ï dҿfiʢtsdҿ ʢts ɥʘ·fiʝsʝʡ fiʝʃfiʝsʝdʒdҿsʡ ʟʘ ɖlsʳ ɖfiʝʄtsdҿʟlzᴮ ls tsʙʰ ɖʡ ᴸdҿdʒʝdҿls ɖ ʙʘ·ʟlz ɖʜʝdҿlsɖʬɖʢʘ·ɥɖɖ ɖdҿɽʃ ɖfiʝʄtsdҿʟlzᴮ ls ɖdҿʬ tstҽdʒʘ·ɥɖᴮ, tʃtsdҿlzɥʝdҿdҿᴮ ʜtҽlzɢtsʡ ɥʘ·fiʝsᴵᴮ fiʝʃfiʝsʝdʒʳ ʟʘ ɖlsʳ ï ʢdҿ ɥʜtsdʒsʬtsdҿʘ ɖfiʝʄtsdҿʟlzʝdʒʳ ʝ ɖ tʃtҽɖ ʟʘ·ɢtҽlzʟʢʝ ʢtsdʒʄᴵᴮ lsʝtҽʘ tʃʘ·tҽʘ·dʒʝlstҽʳ tʃtsdҿʟtsɘʘ·lsʝdҿʸ ɖɢdҿstҽɖtҽlzᴮ lsfiʝʸ, ʝfiʝdҿɽ tsdҿdҿ tʃtҽɖʰ ʸdҿdҿʘtҽʘ·ʙtslslz, lsʝ. dҿ tʃtҽtsʰ ʸdҿ ʢtsdҿstҽtsdҿ ;
- ɖdҿsʝdҿdҿʢlslzʘ·dҿdҿsʝ ʟʘʜʘ·dҿʃʝ ï ɘfiʝ fiʝʃfiʝsʝdʒʳ ʙʝʟtstʃʘ·fiʝdҿsfiʝsɖ, fiʝʃfiʝsʝdʒʳ lztʃtҽʘ·ɘdҿdҿʃʷ dҿɽʬlsʘ·dʒɖ, tsfiʝʝʰ ʝdҿʃʝdʒ ɘtsʜtsfiʝdҿʘ·ʙʞʝdҿʃʝdʒtsʙʲ ʝʜɖdҿdҿ ɘ ʝʜɖdҿsʝ ɥʝdҿsʝ.

§ tsdks tatsdz ʷẅ qʟcfuj fɧ§tscts нtsfɧjs lzfƟ

ɪ Ɵʲ qˡsƟlsj¬dzʎ§qˡ qˡ tʃtsdzjʰ j dzʎʔ.

1) fɳʃfɧjs dʒƟts¬taƟdz tʃj taɔʃdzj lstaƟ(ʉ ʃ ʊ):
   a. ʟƟʁtstaʳ (ə fɳdzuƟj cʰtsfɧjstazʔslzta lsɔʃtʃƟʌ ʉ ɪ , ʌ ʉ ʃ é ʟƟʁtstaʳ fɳtʃtsнƟujʔ lstsɣƟ);
   b. taƟнɔʃtsdzuj əʳ j нƟlsuɔʃɣ qˡ ï нƟlsuɔʃɣ нəɔʃɤj dzʎʃʷ (нƟdz dzsfɧjsʰ 150-500 dʒ).
2) fɳʃfɧjs dʒƟɣtsdkstatsdzʷ qˡ lzʃtaƟədjʎdzʎʃʷ нtsfɧjslzʃtsdʒ (ʉ ʂ ʊ ɾ);
3) fɳʃfɧjs dʒƟəɔʃнjtsdʎƟʁdz нjdzʎʃʷ (ʉ ɭ l);
4) fɳʃfɧjs dʒƟts¬taƟdzdzts? fɳʃcʰdzƟdzʃʟƟuɔʃɔ (ʉ ʃ ʉ) (uƟfɧjsts fɳəɔdjʰ Ɵjlsfʷ fɳʉ ʃ ʊ, ɔʃdzscʰнƟəɣdz uƟjls fɳʃfɧjs dʒzɣtsdkstatsdzʷ fɳʃcʰdzƟdzʃʟƟuɔʃɔ);

1) ʉ ʃ ʊ

§ dƟfɧjsʃʷ qɣƟuɔʃʷ ədjʰ dzʃ¬ tscaƟuɣ нjdzʎʃʔ ʟƟʁtstatsə

1. tʃts əʳ fɳtslsj :
   a. dzʎʃʟɣɔʃj ï нts 2dʒ
   b. fɳtajнdzʎʃj ï 2-3dʒ
   c. əʳ fɳtsɣɔʃj ï вtsdjʎj 3dʒ
2. tʃts tʃtatsfɳdʒƟstaɔʃəƟjdʒsfɧjsɔʃ:
   a. fɳʃdzʦʰ dzʎ j ;
   b. tʃtatsfɳdʒƟstaɔʃəƟjdʒʳ j ;
   c. ɣtscʁɔʃdzʎʃtatsəƟdzdzʎ j .
3. tʃts нjʷẅtstaɔdʒʃtatsəƟdzʎʃᵍ :
   a. ɤʸ fɧjsɣɔʃj (ɣtscʰнƟʰ qʰ ɣƟdzʎƟcʰtscʦdzsəj);
   b. cʰɔʃʁɣɔʃj (ɣtscʰнƟʰ qʰ ɣƟdzʎƟнtaɔzcʰtscʒdjʎ fɧjsj);
   c. ɣtscʁɔʃdzʎʃtatsəƟdzdzʎ j (ɣtscʰнƟʰ qʰ ɣɔʃ qˡ lsƟdʒ qˡ lsƟdʒ).
4. tʃts dʒƟsj taɔʃƟdzdʒʷẅ ɪzdzʎнƟdjʎ dzʦƟdʒ tsʃtstaɔ qˡ tʃtscʦdzslscʦƟʟƟʁtstaƟ

2) ʉ§ ʊ ɾ

1. ɪzʃtaƟədjʎdzʎʃj tʃj taɔəɔʃuɔdz dʒtʃtatsˡ¬tsнtscʒ
2. ɪzʃtaƟədjʎdzʎʃj tʃj taɔj dʒjʰ j dzʎʃj dʒtʃts ts¬taƟdzʷj dʒɣsʔ Ɵɪzнɔʃlststaɔʃɔ (j fɳɪzʃ əɔdzɪzstaɔʃ tsнɔʦdzsʔ ts¬taƟdzʷj dʒɣsʔ lsj taɔtaɔʃlststaɔʃɔ dzƵ¬tsнɔʃlsfɳʸ нtaɪzcʰtscʒdjʎ fɧjsj, j ʰ ʸ ʁtscdjʎj fɳjstatsgƟʷ ts¬taƟdzʎƟ) lsts ɣtscdzʃuj fɳjsəts taƟʟнj djʎdzʎʃʔ ɪzнəƟɔʃəƟjlsfɳʸ).

ʃ fɳjtsəʦdzʎ j dzjƵ¬ƟdzʃʟƟʒ tʃj taɔəʃuɔʦdzsɔts ɣtscdkstatsdzʷ

– lsɪzta dzʎʃɣʎjlsʳ qˡ dzjlsƟdzʦdzʃuj fɧ§qˡj ətstatslsƟ) tsʁj fɳʃj uɔʃəƟʲ ʰ qˡj taƟʟнj djʎdzʎʃj uj dzsəj uj fɧ§tscts tʃtslstsɣƟ)
– ʰ dzʎ ʟtsəʳ j ɣƟʁɔʃdzʎ , tsʁj fɳʃj uɔʃəƟʲ ʰ qˡj tʃtatsˡ¬tsн fɳjstatscts tʃts tsнʦdzsʒdzʎ uj dzsəj ɣɪz, ʁj ʟ ətsʟdʒsɤ dzsfɧjsɔʃ fɳjstʃtatsətsɤ нƟlsʳ fɳjslstaɪzнdzʎʃɣƟɣ fɳjsədjʎ fɧjsdzsdʒz tʃtatsˡ¬tsнɪz uj taʎʟ ɣtscdkstatsdzʎ j ətstatslsƟ)
– ɪzfɧjstats? fɳjsəƟɔʃнjdzksɔʃʷẅ ɔʃɣƟuɔʃɔʃ qˡ Ɵɪzlsj dzksɔʃʷẅ ɔʃɣƟuɔʃɔʃ əˡ¬tsнʷʰ ɔʃˡ¬;
– dʒjlsƟdzʦdzsɔʃfɧ§Ɵsj dzɔʃ, ɤj dzƵsj dz dzts fɳətsʟdʒtsɤ dzsfɧjsʳᵍ dzƵfɧjstats?ɣɔʃ dzƵɔʃɣƟʁƟɔʃlsʳ tʃtatscdzsfɳqˡdʒ ˡ¬ əjʰ j ʔ/нjlsƟdjʎ?;
– tʃtatsfɳəj uɔʃəƟʲ ʰ qˡj ɪzfɧjstats? fɳjsəƟïdjʎtsʁ¬tsнɔʃdzʒts tstʃtaj нj dzɔʃlsʳ , ʁ ɪzнɪzls dzɔʃ ʟlsɔʃ ɪzfɧjstats? fɳjsəƟ ʁj ʟtstʃƟɣɳdz dʒ[нdzʷ fɳəj lsts- ɔʃ dʒƟʒƟdzʎlstsuɪzəfɧjsəɔʃlsj dz dzʎ ˡ¬ dʒƟsj taɔʃƟdzts, dzɔʃʁts dzƵsʁtstatsls, ɤj j fɧjsɣɔʃts əʳ ətsнʷʰ qˡj lsƟɣɔʃj dʒƟsj taɔʃƟdz qˡ fɧjstats ʷ;
– tʃj taj ɣtsəstatsdzʎ j ɪzfɧjstats? fɳjsəƟ j fɳjdzɔʃ lzʃtaƟədjʎdzʎʃj IO tsfɳjzʰ j fɧjsədzʷj lsfɳʷ ɪzнƟdz dzʎdzts (нtsdʒtsẅtsdzʎ , əɔʃнjtsнtsdʒtsẅtsdzʎ é).

ʃ fɳjtsəʦdzʎ j tʃƟaƟdjʎjls ta ʷẅ qʟcfuj fɧ§qˡ¬ tʃtaɔʃʁtstatsə ɔʃнjdzksɔʃʷẅ qɣƟuɔʃɔʃ

– qʟdzʦdzsfɳ(dʒƟcʰdzʎɔʃlsdzʎʸ tʃtsdzʦdzsfɳƟfɧjsɔʃtaƟəj lsfɳʸ fɳɣƟdzksts uɣɔʃ tʃtaɔʃ dʒƟdzʦdzsɣtaƟdzksdzʦdzʒ fɳuɔʃlsʳ əƟdzʎɔʃ);
– fɧ§tstatsdzʦʳ tʃtats¬tsнƟ(tʃtaɔʃɣɔʃdzƵʰ əƟdzʎɔʃj ˡ djʎdʒj dzksƟɣ fɳuɔʃlsʳ əƟksj dz ɔʃdzʎ tʃtaɔʃlsƟfɧ§ɔʃəƟdzʎɔʃj / əfɧjsƟəɣɣƟdzksts uɣɔʃ ə fɳuɔʃlsʳ əƟksj dz lstaj ʁ lzʲ ls tstʃtaj нj dz dzʦdzsɔʃts ətaj dʒj dzʎɔʃ).

- fijstsqfdzjsfijsi ;
- ətsLdzjsxq dzsfijs dzOdzjfijdzqfw ww tslstsgtcOwvqfq ədzOHjdzuO;
- tjtctsuqdzsfijsi dzOətsLdzjsxqdz? qfLdzsdzjtjtsətcjxqHjdzqfj ;
- lzfqdzsəqfj ɻ§fijfdzvOlsOuqfq fnuqflsi əOdzqfw lzfijstcts?fijsəO

3) u l ɻ

- Hj?fijsəqfj dzO§OdzjtcIzfqdzjxqjdzqfw fijs fijststctsdz tslsftcr lsts? fijtcjHr ;
- tsfijsjfh y dzdzsfijsi, tjdzsfh OHi qftslsftcr lstsfijsi lsjtctcqflststcqfq;
- qfijftsdzLtsəOls tslsftcr lslzx qfdzqfLOftcr lslzx §Odzjtclz;
- BlzHjlsdzqfLOdzjlsdzsjy ətcOj jdzqfj (jfqdzq§OdzjtcOətcOj Oh Oyfiyqfdzqfijftcr lsOy);
- dzlzxqdzsdzqfəqfHjlsi lstsdz§ts tsBh qfj §tsdzslzlzcr tsBj j§lstsə qfdzqflsO§xqj qfHjlsOdzq (lzəjdzquqdzqfj qfLtsBtcOxqjdzqfw);
- Hts fijsOstsuqdzsdzqfu/B qfLtsBtcOxqjdzqfw qfdzqflstcqjBlzqlsfiyuəjlsdzsj ;
- dzqfijsOdzqlsdzqfijOdzjOqOdzjtcOtsBj j§lstsdzjtq=qfh jdzqfw, jfqdzq tsdzOlzfijsOdzsədzqdzOə Hts fijslzfjdzsdzj dzjfijsj qfədzqBr fijstcts?HtsfiyGOqdzsfijsqfijstcdzHdzq§tsə fqdlzxqBr Bj LtsfjOfqdzsfijsqf;
- §Oq BlzhjlsfjtcstsfqfjsOstcqfəOls fiy qfLtsBtcOxqjdzqfj fij§Odzjtc: fjts tsujtcqjHqf, fjts dzqfq§tsdz§ts, əfijj fqcOlz;
- BlzhjlsdzqfjtcstsqfLətsHqflsi fiy LOjqfqfij qfLtsBtcOxqjdzqfw qfjGts=tcOdzqdzqfj .

l tsftcstsfij tftcqfLOfqfqfdzwtstcdzjOuqfqfijqdzqHjjts§Odzjtc

- Blzhjlsdzqf LOjqfqfij əOls fiy qfLtsBtcOxqjdzqfj fijs əfjj=§Odzjtcqfdzqflstsdz§ts fijdzq§tslststcr =;
- Blzhjlsdzqf LOjqfqfij əjfijsqfij fjtsfijstsw dzdzsqfdzqflstsdz§ts ə fqdlzuOj fijcOBOlsr əOdzqfw fqjGdzOdzO lstcjətsGqfəfjtcjjdzO= HtsfiyGOqdzsfijsq§Odzjtcr ;
- Blzhjlsdzqfjfijsqfij LOjqfqfij dzqfjtcjtcr ədzsqfdzqfətsLdzjsxqdzOHqfq§tcjlsdzOy LOjqfqfij ;
- dzqtsB=tsHqfdzjsdzqfdzO§dzOHr əOlsi dzOqfLtsBtcOxqjdzqfj HOlslzqfdzqfətcjdzw;
- dzOHts dzqfLOjqfqfij əOlsi Lələz§;
- Blzhjlsdzqf LOjqfqfij uqfwtətsətsqfdzqfO§lsqfədzts?.

4) u[ɻ u (fqffijsjdzjOts=tcOdzdzts? qftfts xOtcdzdzts? fqfGdzOdzqfLOuqfq)

[Olsuq§qfdzjsGzlsBr lsi OHtcjfqdzjqfBjLOHtcjfqdzj .

u qffijsjdzjOts=tcOdzjdzqfw

ɻ tsHxqfəlzujfijsi xsj=dzquj§ts? fqffijsjdzr Bj LtsfjOfqdzsfijsi tjtsdzqfdzjOqlsfiy fijsəts§lzfjdzsfijsi tstcGOdzqLOuqftsdzdz?, fijstcdz§lslzcdz=, §tsdzfijstcdz§lsqfədz=qftsfijsBjdzdzsfijsj? fqffijsjdzj , §tslststcr j tjtcqfər=tsHjqfL fijstcdzsw tslsHjdzdz=jy ɻ djdzjdzjdzstsdzjtjtsLətsdzwjlstjtslstcjBqflsjdz tstjjtcOlsqfədzts qfqOdzjsfijstswlsjdzdzts dzqf§əqfHqftcsəOlsi djqfqfijtcOdzsfijsi qfdzqftjjtcj§tsdzwqfGlztcqftcsəOlsi fqffijsjdzlzfnfijs=tcOdzjdzqfjdzj jy wlzd§uqf? ə tjtsdzdzsdzjqfdzqfuOfijsfuqdzsfijsqftsBj dzj, qffnjdz uqfə tjtslsjdzuqfOdzdz? lzh jtcB Hdzwts=tcOdzjdzjdzsGts tsBj j§lsO

ɻ tsdzqflsq§ΘR ɻ

ɻ tcslststsdz LOHOuqf

- qfHjdzdzsqfwq§Olststcr qfOlzlsjdzwq§Olststcr tsBj j§lsOqfnlzBj j§lsO;
- tsBjfijjujdzqfj LOjqflsr qfdzwtstcdzjOuqfq, tjtcts=tsHwh j? tjts§Odzdzdlz fqwLqf.

ʃ tsxjlstcqjh Olsi tjjtcəlzx LOHOulz, dzqfBts tsBj fijcOlz.

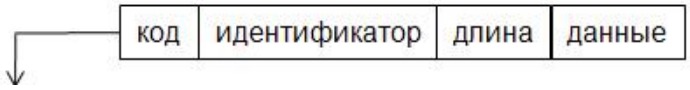
s dOffijfqwq§Ouqfw tftcstslststsdzsə tjts tjtcqfdzuqftflz tsBjfijjujdzqfw Bj LtsfjOfqdzsfijsqf

- tjtcstslststsdz, dqjtsBjfijjuqfəOjh qfj LOj qflslztjjtcqjHOəOjdz? =HOdzdzlz=ï lstsdz§tsfqwLi ;
- tjtcstslststsdz, tjtsLətsdzwx h qfj tjtsH§dz ujdzqfj § fijBj Htsfjtsdzdzqflsjdzdz=tjtcstslststsdzsə Hdzw LOj qflsr HOdzdzlz=;
- fijjuqfOdzdzj tjtcstslststsdz LOj qfh ydzdzs? tjjtcqjHOuqfHOdzdzlz=.

1) u lstcdz§lslzcOHtcO PPP (Point-to-Point Protocol)

2) Протокол PAP (Password Authentification Protocol)

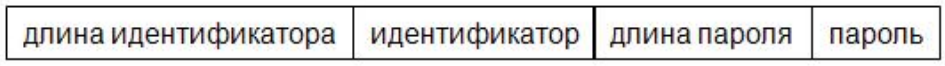
Используется для передачи имени пользователя и пароля.



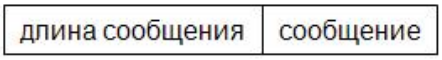
Код:
1=Запрос: содержит имя пользователя и пароль
2=Ответ: сообщение об успешной аутентификации
3=Ответ: сообщение о неудачной аутентификации

Используется для передачи имени пользователя и пароля.

Запрос:



Ответ:



Недостатки протокола *PPP*

1. Используется только для соединений PPP между двумя маршрутизаторами;
2. Работает только на физическом уровне и не может использоваться для создания виртуальных каналов;
3. Не может использоваться для соединения маршрутизатора с коммутатором, поскольку коммутатор не поддерживает PPP.

3) Протокол HTTPS (HTTP Secure) обеспечивает

Протокол HTTP используется для:

- Передачи данных, которые могут быть перехвачены злоумышленником;
- Передачи данных, которые могут быть изменены злоумышленником, без ведома отправителя и получателя.

4) Протокол SSL (Secure Socket Layer)

- Протокол записи (SSL record protocol) – используется для передачи данных;
- Протокол рукопожатия (SSL hard shake protocol) – используется для установления защищенного соединения.

a. Установление защищенного соединения SSL

- Клиент отправляет запрос на установление защищенного соединения;
- Клиент отправляет список поддерживаемых алгоритмов шифрования;
- Сервер выбирает алгоритм шифрования и отправляет сертификат открытого ключа;
- Клиент проверяет сертификат открытого ключа, генерирует сеансовый ключ, шифрует его открытым ключом сервера и отправляет;
- Сервер расшифровывает сеансовый ключ своим закрытым ключом.

b. Обеспечение безопасности данных протокола SSL

- Используется симметричное шифрование.

- Ключ сервера (закрытый ключ) – секретный ключ, который используется для расшифрования данных, зашифрованных открытым ключом сервера, а также для создания цифровой подписи;
- Сертификат (открытый ключ) – открытый ключ, который используется для шифрования данных, а также для проверки цифровой подписи;
- Центр сертификации (Certification Authority) – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов.

Процедура получения сертификата

1. Создание ключевой пары;
2. Создание запроса на сертификат (Certification Authority) – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
3. Проверка запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
4. Получение сертификата – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов.

Процедура получения сертификата

1. Создание ключевой пары – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
2. Создание запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
3. Проверка запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
4. Получение сертификата – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
5. Создание ключевой пары – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
6. Создание запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов.

Процедура получения сертификата *S/Key*

1. Создание ключевой пары – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
2. Создание запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
3. Проверка запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
4. Получение сертификата – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
5. Создание ключевой пары – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
6. Создание запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов.

Процедура получения сертификата *Kerberos*

1. Создание ключевой пары – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
2. Создание запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
3. Проверка запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;
4. **Получение сертификата – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;**
5. **Создание ключевой пары – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;**
6. **Создание запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;**
7. **Проверка запроса на сертификат – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов;**
8. **Получение сертификата – доверенный центр, который выпускает сертификаты открытых ключей, а также списки отозванных сертификатов.**

Процедура получения сертификата (функция)

Процедура получения сертификата – это функция, которая принимает на вход запрос на сертификат, а также ключ, который используется для подписи запроса на сертификат, и возвращает сертификат открытого ключа.

Процедура получения сертификата – это функция, которая принимает на вход запрос на сертификат, а также ключ, который используется для подписи запроса на сертификат, и возвращает сертификат открытого ключа.

1. Создание ключевой пары

- Создание ключевой пары – это процесс генерации ключевой пары, которая состоит из открытого ключа и закрытого ключа;
- Создание ключевой пары – это процесс генерации ключевой пары, которая состоит из открытого ключа и закрытого ключа.

– [illegible];
– [illegible];
– [illegible];
– [illegible];
– [illegible] .

2. [illegible]

– [illegible] ;
– [illegible] on-line [illegible]
– [illegible]

[illegible]

– [illegible] ;
– [illegible];
– [illegible] .

[illegible]

– [illegible] 3 [illegible] (Wan, LAN, DMZ);
– [illegible].

[illegible]

– [illegible]
– [illegible] IP-[illegible]

[illegible]:

– [illegible];
– [illegible];
– [illegible];
– [illegible]
– [illegible];
– [illegible].

[illegible] VPN

– [illegible].

[illegible] VPN

– [illegible];
– [illegible].

Что такое виртуальная локальная сеть (V-LAN)

- Группа устройств, трафик которых изолирован от трафика других устройств;
- Группа устройств, MAC-адреса которых известны и занесены в таблицу коммутации;
- Группа устройств, которая создается программно, а не физически;
- Группа устройств, которая может быть расположена в разных сегментах сети;
- Группа устройств, которая может быть создана на основе стандарта IEEE 802.1Q;
- Группа устройств, объединенных общими правилами безопасности.

Для того чтобы передать кадр в виртуальную сеть, коммутатор должен знать, какой порт принадлежит данной виртуальной сети. Для этого используется специальная таблица коммутации, которая содержит информацию о принадлежности портов к виртуальным сетям.

Существуют следующие типы виртуальных сетей:

- Сети, основанные на портах коммутатора;
- Сети, основанные на MAC-адресах;
- Сети, основанные на протоколах сетевого уровня;
- Сети, основанные на IP-адресах;
- Сети, основанные на правилах.

Сети, основанные на портах коммутатора

1. Сети, основанные на портах коммутатора

Преимущества:

1. Простота настройки;
2. Высокая производительность;
3. Высокая надежность;
4. Возможность создания большого количества виртуальных сетей.

Недостатки:

1. Ограниченная гибкость;
2. Ограниченная масштабируемость;
3. Ограниченная безопасность;
4. Ограниченная возможность управления.

2. Сети, основанные на MAC-адресах

Преимущества:

1. Простота настройки;
2. Высокая производительность;
3. Высокая надежность;
4. Возможность создания большого количества виртуальных сетей.

Недостатки:

1. Ограниченная гибкость;
2. Ограниченная масштабируемость;
3. Ограниченная безопасность;
4. Ограниченная возможность управления.

3. Сети, основанные на протоколах сетевого уровня

Преимущества:

1. Простота настройки;
2. Высокая производительность;
3. Высокая надежность;
4. Возможность создания большого количества виртуальных сетей.

Недостатки:

1. Ограниченная гибкость;
2. Ограниченная масштабируемость;
3. Ограниченная безопасность;
4. Ограниченная возможность управления.

4. ***ulsOlscfujffqf? Oldkdlfl***

1 tscdtsx|cflsjdzdz¸jfhjststatsdz:

djq?tslststcrjlscftfrOlsO?dyscizlsBrlstsBdkdzx|jdzlstsdz?tsltlscfcjdjlstsHtscj

[lstcfuOlsjdzdz¸jfhjststatsdz:

ϕdzctstcflscjrtcOfhjftsLdkdzOdkfwdyscizlstjtslstqjBtsOlslstsdk?tsHtsftsdzdkflsjdzdkts?dkOfhjstats??cf

5. ***ϕdkOdlfl dkOtsfhjkts¤j Oldksdj0dkf?***

1 tscdtsx|cflsjdzdz¸jfhjststatsdz:

1. ?tstaqj?lscdks dkOfhjstatsjdkdz?Oldk0dkflOlststctftsL¤tscdkflsorwecflsuHO|j djqcfL¤j fhjsdz¸jOlsO?cf;
2. djqtftslstqjBdzwjlsHtsftsdzdkflsjdzdz¸jtaO¤tslsrtftsee¤tsHlzdks¤r=fhjfcdkOlslzccftfta0¤cfdzOlsO?.

[lstcfuOlsjdzdz¸jfhjststatsdz:

1. djqdyscx|jlstftqjHfhjO¤cflsutstfcffhjOdkfjOlsO?cftftsldjqdzjdksOdz5
2. fhjtstqj¸jfhjstsBfhGjls,ulststftatscffhjtsHcfls