

Áðþñ Øí àéáð

Ī ðèêëääí àÿ êðèì òîãðàôèÿ

2-à èçääí èà

Ī ðîòîêîëû, àëãî ðèòî ù è èñòîáí ùà òàèñòù í à ÿçûêà Ñ

ÑĪ ÄÅÐÆÀÍ ÈÅ

Óèòòèèä Äèòòè. Ī ðãàèñèí àéà

Åãääáí èà

Ãèääà 1

Ī ñí îáí ùà ï îí ÿòèÿ

- 1.1 Òaðì èí îêîãèÿ
- 1.2 Ñòääáí îãðàôèÿ
- 1.3 Ī îñòàí îáí-í ùà è ï àðãñòàí îáí-í ùà øèòðù
- 1.4 Ī ðîñòí à XOR
- 1.5 Ī áí îðàçîáúà áéí èí îòù
- 1.6 Êîí ï ïþòàðí ùà àëãî ðèòî ù
- 1.7 Áí èüøèà -èñèà

×àñòù Ī Êðèì òîãðàôè-àñèèà ï ðîòîêîëû

Ãèääà 2

Ýèàì áí òù ï ðîòîêîëèà

- 2.1 Åãääáí èà á ï ðîòîêîëû
- 2.2 Ī àðããà-à èí òîðì àòèè ñ èñí î èüçîááí èàì ñèì ï àòðè-í î é èðèì òîãðàôèè
- 2.3 Ī áí îí áí ðãàèáí í ùà òîí èòèè
- 2.4 Ī áí îí áí ðãàèáí í ùà òÿø-òîí èòèè
- 2.5 Ī àðããà-à èí òîðì àòèè ñ èñí î èüçîááí èàì èðèì òîãðàôèè ñ îðèòùòù è èþ-àì è
- 2.6 Õèòðí áúà ï îáí èñè
- 2.7 Õèòðí áúà ï îáí èñè è øèòðí ááí èà
- 2.8. Ááí àðãòèÿ ñèó-àéí ùò è ï ñããáí ñèó-àéí ùò ï ï ñèãáí ààòàèüí î ñòáé

xañòù II Êðèi òí ãðàÒè÷ãñèèá ì áòí äù

Ãèàà 7

Äèèí à èëþ÷à

- 7.1 Äèèí à ñèì ì àððè÷í îãí èëþ÷à
- 7.2 Äèèí à îðèðùòíãí èëþ÷à
- 7.3 Ñðãáí áí èà äèèí ñèì ì àððè÷í ùð è îðèðùòíð èëþ÷àé
- 7.4 Æñèðùðèà á ááí ù ðí æãáí èý ì ðí òèá îáí îí àí ðããéáí í ùð òýø-òóí èöèé
- 7.5 Êãèí á äí èæí ù áùòù äèèí à èëþ÷à?
- 7.6 Caveat emptor

Ãèàà 8

Óí ðããéáí èà èëþ÷àì è

- 8.1 Ááí áðãöèý èëþ÷àé
- 8.2 Í äèèí áéí ùá ì ðí ñòðáí ñòãã èëþ÷àé
- 8.3 Í áðããã÷à èëþ÷àé
- 8.4 Í ðí áãðèà èëþ÷àé
- 8.5 Êñí î èüçíããí èà èëþ÷àé
- 8.6 Í áí îãéáí èà èëþ÷àé
- 8.7 Òðáí áí èà èëþ÷àé
- 8.8 Ðãçðáí ùá èëþ÷è
- 8.9 Ñèí ì ì ðí ì àðèðíããí í ùá èëþ÷è
- 8.10 Áðáí ý æèçí è èëþ÷àé
- 8.11 Ðãçðóáí èà èëþ÷àé
- 8.12 Óí ðããéáí èà îðèðùòí è èëþ÷àì è

Ãèàà 9

Òèí ù äèãíðèòí îá è èðèí òíãðàÒè÷ãñèèà ðãæèì ù

- 9.1 Ðãæèì ýèãèððíííé è èððíããèüííé èí èãè
- 9.2 Í îáòð áéí èà
- 9.3 Ðãæèì ñòãí èáí èý áéí èí á èèððà
- 9.4 Í îí èí áùá èèððù
- 9.5 Ñàì î ñèí òðí í èçèððþùèãñý ì îí èí áùá èèððù
- 9.6 Ðãæèì îáðãòíé ñãýçè ìí èèððó
- 9.7 Ñèí òðí í ùá ì îí èí áùá èèððù
- 9.8 Ðãæèì áùòí áí íé îáðãòíé ñãýçè
- 9.9 Ðãæèì ñ÷àð÷èèà
- 9.10 Äðóèèà ðãæèì ù áéí ÷í ùð èèððí á
- 9.11 Áùáí ð ðãæèì à èèððã
- 9.12 Í ðí ñèèèããí èà
- 9.13 Áéí ÷í ùá èèððù ì ðí òèá ì îí èí áùð èèððí á

Ãèàà 10 (Òãñò ãèããù í à áí äèèíèí ì , sorry. Í áðããí ä÷èè, ì òí æã, òñðàè :-)

Êñí î èüçíããí èà äèãíðèòí îá

- 10.1 Áùáí ð äèãíðèòí à
- 10.2 Êðèí òíãðãöèý ñ îðèðùòí èëþ÷í ì ðí òèá ñèì ì àððè÷íé èðèí òíãðãöèè

- 10.3 Øeððí áái eá eí ì ì óí eèàöeí í í ùõ eáí aei á
- 10.4 Øeððí áái eá oðái eí ùõ áái í ùõ
- 10.5 Áí í aðaóí í á øeððí áái eá í ðí ðeá í ðí aðaí ì í í áí øeððí áái eý
- 10.6 Êí ì ì ðaíñeý, eí æeðí áái eá e øeððí áái eá
- 10.7 Áúýaéái eá øeððí áái eý
- 10.8 Ñeðúòeá øeððáeíñá á øeððáeíñá
- 10.9 Ðaçðóðái eá eí oí ðí àøeè

× añòù III Éðeí oí aðà Õe÷ añeèá àeáí ðeòì Ù

Ãeààà 11

Ì àòàì àòe÷ añeèá í ñí í á ù

- 11.1 Óaí ðeý eí oí ðí àøeè
- 11.2 Óaí ðeý ñeí æí í ñòe
- 11.3 Óaí ðeý ÷eñæ
- 11.4 Ðaçeí æaí eá í à ì í í æeðáeè
- 11.5 Áaí aðaöeý í ðí ñoí áí ÷eñeá
- 11.6 Æeñeðáoi úa eí áaðeòì ù á eí í á÷í ì í í eá

Ãeààà 12

Ñòàí áaðò øeððí áái eý áái í ùõ DES

- 12.1 Ááááái eá
- 12.2 Í í eñái eá DES
- 12.3 Áaçí í ñaí í ñòù DES
- 12.4 Æeðóaðaí øeaeíí úe è eèí aéí úe eðeí oí áí aèç
- 12.5 Ðaaeíí úa eðeðaðeè í ðí aèeðí áái eý
- 12.6 Áaðeáí oú DES
- 12.7 Í añeí eüeí áaçí í ñaí ñaí áí ý DES?

Ãeààà 13

Äðóãeá aei ÷ í ùá øeððú

- 13.1 LUCIFER
- 13.2 MADRYGA
- 13.3 NewDES
- 13.4 FEAL
- 13.5 REDOC
- 13.6 LOKI
- 13.7 KHUFU è KHAFRE
- 13.8 RC2
- 13.9 IDEA
- 13.10 MMB
- 13.11 CA-1.1
- 13.12 SKIPJACK

Ãëàà 14

È àúà í áëí÷í ûõ øèòðàõ

- 14.1 ÃĪ ÑÒ
- 14.2 CAST
- 14.3 BLOWFISH
- 14.4 SAFER
- 14.5 3-WAY
- 14.6 CRAB
- 14.7 SXAL8/MBAL
- 14.8 RC5
- 14.9 Äðóãèà áëí÷í ûà àëãĭ ðèòĭ û
- 14.10 Òãĭ ðëÿ ĭ ðĭ àèòèðĭ àãĭ èÿ áëí÷í ĭãĭ øèòðà
- 14.11 Ēñĭ ĭ èüçĭ àãĭ èà ĭãĭ ĭ ĭ àĭ ðààèãĭ ĭ ûõ ðÿø-òóĭ èöèè
- 14.12 Âúãĭ ð áëí÷í ĭãĭ àëãĭ ðèòĭ à

Ãëàà 15

Î áúãèĭ áĭ èà áëí÷í ûõ øèòðĭâ

- 15.1 Äãĭ éĭ ĭà øèòðĭ àãĭ èà
- 15.2 Òðĭ éĭ ĭà øèòðĭ àãĭ èà
- 15.3 Óããĭ áĭ èà äèèĭ û áëíèà
- 15.4 Äðóãèà ñòãĭ û ĭ ĭ ĭãĭ èðãòĭ ĭãĭ øèòðĭ àãĭ èÿ
- 15.5 Óĭ áĭ üøãĭ èà äèèĭ û èèĭ÷à à CDMF
- 15.6 Ī óããèèãĭ èà
- 15.7 Ī ĭ ĭãĭ èðãòĭ ĭà ĭ ĭ ñèããĭ ààòãèüĭ ĭà èñĭ ĭ èüçĭ àãĭ èà áëí÷í ûõ àëãĭ ðèòĭ ĭà
- 15.8 Ī áúãèĭ áĭ èà ĭ àñèĭ èüèèð áëí÷í ûõ àëãĭ ðèòĭ ĭà

Ãëàà 16

Ããĭ àðãòĭðû ĭ ñãããĭ ñèó÷àéĭ ûõ ĭ ĭ ñèããĭ ààòãèüĭ ĭ ñòãé è ĭ ĭòĭèĭâúà øèòðû

- 16.1 Èèĭ áéĭ úà èĭ ĭ ãðóÿĭ òĭ úà àãĭ àðãòĭ ðû
- 16.2 Ñããèãĭ âúà ðããèñòðû ñ èèĭ áéĭ ĭ é ĭ àðãòĭ ĭ é ñãÿçĭĭ
- 16.3 Ī ðĭ àèòèðĭ àãĭ èà è áĭ àèèç ĭ ĭ òĭ èĭ âúò øèòðĭ à
- 16.4 Ī ĭòĭ èĭ âúà øèòðû ĭ à àãçà LFSR
- 16.5 A5
- 16.6 Hughes XPD/KPD
- 16.7 Nanoteq
- 16.8 Rambutan
- 16.9 Äããèðèãĭ úà àãĭ àðãòĭ ðû
- 16.10 Gifford
- 16.11 Äëãĭ ðèòĭ M
- 16.12 PKZIP

Ãëàà 17

Äðóãèà ĭ ĭòĭèĭâúà øèòðû è àãĭ àðãòĭðû ĭ àñòĭÿùèð ñèó÷àéĭ ûõ ĭ ĭ ñèããĭ ààòãèüĭ ĭ ñòãé

- 17.1 RC4
- 17.2 SEAL

17.3 WAKE

- 17.4 N̄aaēāi āua ḁaaēñòḁ ŋ ī āḁaōī ī ē n̄āyçūḁ ī ī āḁāī ī ñò
- 17.5 Ī ī ōī ēī āua øēòḁ, ēñī ī ēüçḁḁḁ FCSR
- 17.6 N̄aaēāi āua ḁaaēñòḁ ŋ ī aēēī aēī ī ē ī āḁaōī ī ē n̄āyçūḁ
- 17.7 Āḁóāēā ī ī ōī ēī āua øēòḁ
- 17.8 N̄ēñòāī ī ī -ḁāī ḁaòē-āñēēē ī ī āōī ā ē ī ḁī aēòēḁī āāī èḁ ī ī ōī ēī āuò øēòḁā
- 17.9 N̄ēī aēī ī ñòī ī -ḁāī ḁaòē-āñēēē ī ī āōī ā ē ī ḁī aēòēḁī āāī èḁ ī ī ōī ēī āuò øēòḁā
- 17.10 Āḁóāēā ī ī āōī āu ē ī ḁī aēòēḁī āāī èḁ ī ī ōī ēī āuò øēòḁā
- 17.11 Øēòḁ ŋ ēāñēāāī ī ī añēī ēüēēò ī ī ōī ēī ā
- 17.12 Āuāī ḁ ī ī ōī ēī āī āī øēòḁ
- 17.13 Āāī āḁaòēy ī añēī ēüēēò ī ī ōī ēī ā èç ī āī ī āī āāī āḁaōī ḁā ī ñāāī ñēó-āēī ī ē ī ī ñēāāī āāḁaēüī ī ñòē
- 17.14 Āāī āḁaōī ḁ ŋ ḁaaēüī ŋ ñēó-āēī ŋ ī ī ñēāāī āāḁaēüī ī ñòāē

Ãèàà 18

Ī āī ī ī āī ḁāāēāī ī ŋā òýø-òóī èòèè

- 18.1 Ī ñī ī āu
- 18.2 Snefru
- 18.3 N-òýø
- 18.4 MD4
- 18.5 MD5
- 18.6 MD2
- 18.7 Āēāī ḁèòī āāçī ī āñī ī āī òýøèḁī āāī èy (Secure Hash Algorithm, SHA)
- 18.8 RIPE-MD
- 18.9 HAVAL
- 18.10 Āḁóāēā ī āī ī ī āī ḁāāēāī ī ŋā òýø-òóī èòèè
- 18.11 Ī āī ī ī āī ḁāāēāī ī ŋā òýø-òóī èòèè, ēñī ī ēüçḁḁḁ ñēī ī āòḁē-ī ŋā aēī -ī ŋā aēāī ḁèòī ŋ
- 18.12 Ēñī ī ēüçī āāī ēā aēāī ḁèòī ī ā ñ ī òèḁüòüī èèḁ-ñī
- 18.13 Āuāī ḁ ī āī ī ī āī ḁāāēāī ī ī ē òýø-òóī èòèè
- 18.14 Ēī āu ī ḁī āāḁēē ī ī aēēī ī ī ñòē ñī ī āuāī èy

Ãèàà 19

Āēāī ḁèòī ŋ ñ ī òèḁüòüī è èèḁ-āī è

- 19.1 Ī ñī ī āu
- 19.2 Āēāī ḁèòī ŋ ḁḁçāēā
- 19.3 RSA
- 19.4 Pohlig-Hellman
- 19.5 Rabin
- 19.6 ElGamal
- 19.7 McEliece
- 19.8 Ēḁēī òī ñēñòāī ŋ ñ yēēēī òē-āñēēī è èḁēāuī è
- 19.9 LUC
- 19.10 Ēḁēī òī ñēñòāī ŋ ñ ī òèḁüòüī èèḁ-ñī ī ā āāçā ēī ī ā-ī ŋā āāòī ñ āōī ā

Ãèàà 20

Āēāī ḁèòī ŋ øēòḁī āī ē ī ī āī èñē ñ ī òèḁüòüī èèḁ-ñī

- 20.1 Āēāī ḁèòī øēòḁī āī ē ī ī āī èñē (DIGITAL SIGNATURE ALGORITHM, DSA)
- 20.2 Āāḁēāī òü DSA
- 20.3 Āēāī ḁèòī øēòḁī āī ē ī ī āī èñē ĀĪ ÑÒ
- 20.4 Ñòāī ŋ øēòḁī āī ē ī ī āī èñē ñ ēñī ī ēüçī āāī ēāī aēñēḁaōī ŋ ēī āāḁèòī ī ā

- 20.5 ONG-SCHNORR-SHAMIR
- 20.6 ESIGN
- 20.7 Ēëàòì ÷í ùá ààòì ì àòù
- 20.8 Äðóàèà àëáí ðèòì ù ñ í òèðùòùì èëþ÷íì

Ãëààà 21

Ñòàì ù èäáí òèòèèàòèè

- 21.1 FEIGE-FIAT-SHAMIR
- 21.2 GUILLOU-QUISQUATER
- 21.3 SCHNORR
- 21.4 Ī ðáí áðàçí àáí èà ñòàì èäáí òèòèèàòèè á ñòàì ù ì í äí èñè

Ãëààà 22

Äëïðèòì ù íáì áí à èëþ÷àì è

- 22.1 DIFFIE-HELLMAN
- 22.2 Ī ðí òí êí è "òí ÷èà-òí ÷èà"
- 22.3 Òðáòì ðí òí áí ùé ì ðí òí êí è Øàì èðà
- 22.4 COMSET
- 22.5 Ī áí áí çàøèòðí àáí í ùì è èëþ÷àì è
- 22.6 Çàùèøáí í ùá ì áðááí áí ðù í èëþ÷à
- 22.7 Ðàñì ðááàéáí èà èëþ÷à äëÿ êí í óáðáí òèè è ñáéðáòí äÿ øèðí êí ááùàòáéüí äÿ ì áðááà÷à

Ãëààà 23

Ñì áòèàéüí ùá àëáíðèòì ù äëÿ ì ðíòíêíêíá

- 23.1 Êðèì òí áðáòèÿ ñ í áñêí èüèè è í òèðùòùì è èëþ÷àì è
- 23.2 Äëïðèòì ù ðàçááéáí èÿ ñáéðáòà
- 23.3 Ī í áñí çí àòáéüí ùé èáí àè
- 23.4 Ī áí òðèòááì ùá òèòðí áùá ì í äí èñè
- 23.5 Ī í äí èñè, ì í àòááðæáááì ùá áí ááðáí í ùì èèòíì
- 23.6 Áù÷èñéáí èÿ ñ çàøèòðí àáí í ùì è ááí í ùì è
- 23.7 Áðí ñáí èà "÷áñòí í é" ì í í áòù
- 23.8 Ī áí í í äí ðááéáí í ùá ñòì ì áòí ðù
- 23.9 Ðàñèðùòèà ñáéðáòí á "áñá èèè í è÷ááí"
- 23.10 ×áñòí ùá è í òèàçí òñòí é÷èáùá êðèì òí ñèñòáì ù
- 23.11 ZERO-KNOWLEDGE PROOFS OF KNOWLEDGE
- 23.12 Ñéáí ùá ì í äí èñè
- 23.13 Ī áðááà÷à ñ çááùááí èáì
- 23.14 Ááçí ì áñí ùá áù÷èñéáí èÿ ñ í áñêí èüèè è ó÷áñòí èèàì è
- 23.15 Ááðí ÿòí ì ñòí í á øèòðí ááí èà
- 23.16 Êááí òí áàÿ êðèì òí áðáòèÿ

×àñòù IV Ðààëüí Úé ì èð

Ãèàà 24

Ï ðèì àðú ðààèèçàöèè

- 24.1 Ï ðì òì èí è óì ðààèáí èÿ ñàèðàòì úì è èèþ-àì è èí ì ì áì èè IBM
- 24.2 MITRENET
- 24.3 ISDN
- 24.4 STU-III
- 24.5 KERBEROS
- 24.6 KRYPTOKNIGHT
- 24.7 SESAME
- 24.8 Ï áùàÿ èðèì òì ðààèè-áñèàÿ àððèòàèòòðà IBM
- 24.9 Ñðàì à ì ðì áàðèè ì ì äèèí ì ì ñòè ISO
- 24.10 Ï ì-ðà ñ ì ì áùøáí ì é ñàèðàòì ì ñòùþ PRIVACY-ENHANCED MAIL (PEM)
- 24.11 Ï ðì òì èí è ááçì ì áñì ì ñòè ñì ì áùáí èé
- 24.12 PRETTY GOOD PRIVACY (PGP)
- 24.13 Èí òàèèàèòàèüí úà èàðòì-èè
- 24.14 Ñðàì áàðòù èðèì òì ðààèè ñ ì òèðòùòì è èèþ-àì è
- 24.15 Óì èáàðñàèüí àÿ ñèñòàì à ÿèàèòðì ì ì úò ì èàòàèé
- 24.16 CLIPPER
- 24.17 CAPSTONE
- 24.18 Ááçì ì áñì úé òàèàòì ì AT&T MODEL 3600 TELEPHONE SECURITY DEVICE (TSD)

Ãèàà 25

Ï ìèèèèè

- 25.1 Áááí òñòáí ì àòèí ì àèüí ì é ááçì ì áñì ì ñòè (NSA)
- 25.2 Ï àòèí ì àèüí úé òáí òð èí ì ì ùþòàðì ì é ááçì ì áñì ì ñòè (NCSC)
- 25.3 Ï àòèí ì àèüí úé èí ñòèòòò ñòáí áàðòì á è òàðì èèè
- 25.4 RSA Data Security, Inc.
- 25.5 PUBLIC KEY PARTNERS
- 25.6 Ï áæáóì àðì áí àÿ àññì òèàòèÿ èðèì òì èí ñè-áñèèò èññèááí ààì èé
- 25.7 Ï òáí èà ì ðèì èòèáí á òàèí ñòì ì ñòè RACE (RIPE)
- 25.8 Óñèí áí úé áí ñòòì äèÿ Ááðì ì ú (CAFE)
- 25.9 ISO/IEC 9979
- 25.10 Ï ðì óáññèí ì àèüí úà è ì ðì ì úøèáí ì úà ðòòì ì ú, à òàèæà ðòòì ì ú çàùèòì èèí á ððàæááí ñèèò ñáí áí ä
- 25.11 Sci.crypt
- 25.12 Øèòðì ì áí èè
- 25.13 Ï àòáí òù
- 25.14 Ýèñì ì ðòì ì á çàèí ì ì áàòàèüñòáí ÑØÀ
- 25.15 Ýèñì ì ðò è èì ì ì ðò èðèì òì ðààèè çà ðóááæì ì
- 25.16 Ï ðàáí áùá áí ì ðì ñù

Ï ÿòò Áèáéç. Ï ì ñèáñèí àèá

×àñòü V Èñõî äí Ñá êî äÜ

1. DES
2. LOKI91
3. IDEA
4. GOST
5. BLOWFISH
6. 3-WAY
7. RC5
8. A5
9. SEAL

Áèáëèî ãðàÖèÿ