

Í àēī òī ðŭá āīāī ðŷò, ÷òī Ī èòāāī ð íá īñòāāēē íè íāííāī  
ñī÷èíáíèŷ, íī ííè íøéáàðòñŷ. Āāðāēēèò-òèçèè áāāā èè íá  
ēðè÷èò: "Ī èòāāī ð, Ī íāñàðŝíā ñŭí, çàíèì àēñŷ ñī áèðáíèàì  
ñāāāáíèé áíēüøá āñāō ēðāāé íà ñāàòá è, íííāāāðāāā ñāāá ýòè  
ñī÷èíáíèŷ, áŭāāē çà ñāīð ñī āñòāáííóð ì óäđīñòü  
ì ííāīçíàēñòāī è ì íøáííè÷āñòāī "...

Äēīāāí Èāŷðòèé

İ İ ÒÎ ×Í ŪÅ ØÈÔĐŪ

Đaçóëüòàòŭ çàðóááæí í é í òèđŭòî é  
êðèì òî ëî ãèè

İ îñêâà

1997

# Ï ðàáóáááì èáì èà, ì ìÿñìÿþùáá, èàè è äëÿ ÷ááì í àì èñàì à ÿòà éí èãà

"Ðááì èþòèííí ùá òñí áðè, èì ááøèà ì áñòí á ì ðíøááøèà ááñÿðèèáðèÿ, ì ðáì áðàçí ááèè èðèì òí áðàðèèþ èç ìíèóíáó-ííé àèñòèì èèì ù á ðáñí áèðàááèÿí ùé ðàçááè òáì ðàðè-áñèí é èí ì ìþòáðí í é í áòèè.

Í àøèì í àì áðáì èáì áúèì í àì èñàòù éí èáó, èí òí ðáÿ ì ðááñòááèèà áú áàçí áúá èí ì òáì øèè, ì ðáááèáì èÿ è ðàçóèÿðàðù á èðèì òí áðàðèè"<sup>1</sup>, à òí-í áá - á èí í èðáðí í é áá í áèáñòè, ì ðááòù ááþùáè ì áðí áú ì ì òí-í í áì øè ò ðí ááì èÿ.

"Ááííáÿ éí èãà ì ðááí áçí á-áí á á èá-áñòáá ñí ðááì-í èèà äëÿ ì ðí øáññèí í áèÿí ùð èðèì òí áðàðèí á, çááñù ì í èñàì ù çáñèóæèááþùéá áí èì áí èÿ ì áðí áú è áèáí ðèòì ù, í áðÿáó ñ òáì ðàðè-áñèè è èí ì òáì øèÿì è è áñí ì ì í ááðáèÿí ùì è ì áðáðèáèáì è. Èí èãà ÿáèÿáðñÿ òáèæá í áñòí ÿòáèÿí ùì èñòí-í èèì èðèì òí áðàðè-áñèèð ñááááì èé, ì í èáçí ùð èàè ñòóááì òáì, òáè è ì ðáì í áááðáèÿì.

Í àøáè òáèÿþ áúèì ñí áðáòù ñòù ááñòáóþùéá èðèì òí áðàðè-áñèèà çí áí èÿ á ááèì ùé ñí áèáñí ááì í ùé òí, ì ðèáì èáì ùé èàè äëÿ ñí áòèáèèñòí á-ì ðáèðèèí á, òáè è äëÿ áèáááì è-áñèèð ì áðáì áðèèí á.

Òíðÿ ááííáÿ éí èãà í á ì ðááòñí áððèáááð áá èèí áéííá ÷ðáì èá ñ í á-áèà áí èí ì òá, ì áðáðèáè ì í áí áðáì òáèèì í áðàçí ì, ÷ðí áú è ì í áí áí ùé ì í áðí á í á áúè ááññí ùñèáí í ùì. Ááòí ÿ ì ñí í áí ùì è òáèÿì è, ì ì ðèáèðí ááí í ùì è "ñí ðááì-í í é" ì ðèðí áí é éí èáè, ñòáèè ñèááóþùéá - ì ðááì ñòááèðù èááèèè áí ñòóí è ñáì ì ñòí ÿòáèÿí ùì ðàçóèÿðàðù è í ááñí á-èðù òáì áí í á ñí ì òí áñáì èá áèáí ðèòì í á è òáì ðàðè-áñèèð ðàçóèÿðàðù á. Äëÿ í áèáá-áí èÿ áí ñòóí á è ì áðáðèáèð ì í áðàçááè ù éí èãè ñí ááæáì ù ì ì í áí òðí áí ááì é í òí áðáðèáè."<sup>2</sup>

"Áñÿèí á ñí-èí áí èá, èàè ááèì ÷áèí áá-áñèí á, èì ááð ñáì è í ááì ñòáðèè. ß ì-áí ù çí áþ, ÷ðí ì í é òðóá áí èáá, í áæáèè ì í í áèá áððáèá, áí èæáí, ì ì ñòù ì ñòè ñáí áé, ì í ááðù ì í áí á è ñí ðááááèèá ùì èðèðè-áñèèì çáì á-áí èÿì. Ðàçí ì í áðàçéá ì ðááì áðí á, èí òí ðùá äëÿ ì í èí ì òù áí èæí ù áðí áèðù á ñí ñòáá Èáèñèèí á, òðóáí ì ñòù ñí ðàçí áðèðù í áúáì ñòáðáè ñ ì òí ì ñèðáèÿí ì þ èð ááæí ì ñòù þ è í á òí òñòèðù èç áèáó ááèì ñòáá á èçèí æáì èè, ðáøèðáèÿí áÿ í ááí çí ì æí ì ñòù èç ááæáðù á í áèí òí ðùð ñèó-áÿð ì í áðí ðáì èé, í áí áðááì òáì ì í ñòù í áøááì ì áðáì áðè-áñèí áí ÿçùéá, - áñá ÿòí çáñòááèÿáð ì áí ÿ áòí áðù, ÷ðí í áñí ì òðÿ í á áñá ì í è ñòáðáì èÿ, èí èãà ì ì ÿ ááèáèì áúá í á òáì áèáðáì ðÿáð òñèí áèÿì òí ðí øááì èáèñèèí áðàðè-áñèí áí ðóèí áí áñòáá. Ì í æáð áúðù, ì ðá-áñòáá í ùá ì áðáì áðèèè í áèáóð òáèæá, ÷ðí í áèí òí ðùá òáðí èí ù è ðá-áí èÿ ì áðáááì ù í á ñí áñáì òáá-í í á ì í áì Èáèñèèí á; çáðáì áá ì ðí øó èð áúðù ñí èñòí áèðáèÿí ùì è è òáèèì í ááì ñòáðèèì."<sup>3</sup>

"È áñá æá ÿ ì í èáááþ, ÷ðí í á-ðí í áí í èí í á - ÿòí áñá-ðáèè èó-øá, ÷áì í è-ááì"<sup>1</sup> ...

<sup>1</sup> Í ááá Áí èáðáèð, èç Ì ðááèñèí áèÿ è ì ì óáèèèí ááí í ùì á Internet òðááì áí òáì í ááí ì èñáì í í é éí èáè "Ì ñí í ááì èÿ èðèì òí áðàðèè", 1995 áí á

<sup>2</sup> Á. Ì áí áçáñ, Ì. Ááí Ì ì ðñòí ò è Ñ. Áÿí ñòí óí, "Ñí ðááì-í èè ì ì ì ðèèèááí í é èðèì òí áðàðèè", CRC Press, 1996 á., èç Ì ðááèñèí áèÿ

<sup>3</sup> "Ì ðááóáááì èáì èá" èç "Èáèñèèí á-èñòí é è ì ðèèèááí í é ì áðáì áðèèè" Á. ß. Áóí ÿèí áñèí áí, 1839 áí á.

# ÑĪ ÄĀÐÆĀÍ ÈĀ

## Äëää 0. Ääääí èä

0.1 Äaçĭ ääy òàðĭ èĭ ĭ ĩ ĩ äëy è ĭ áùèä ĭ ĩ ĩ ĩ äáí èy .....	1
0.2 Ēĭ ĭ òáĭ òëy Ðĭ ĭ ĩ äëy ĭ ÷àòùðäò ĭ ĩ äōĭ ääò è èĭ ĭ ñòðòèðĭ äáĭ èĭ ĭ ĩ òĭ ÷ĭ Ûò øèòðĭ ä .....	4
0.3 Ēèäññèòèèäöëy ĭ ĩ òĭ ÷ĭ Ûò øèòðĭ ä .....	6
0.3.1 Ñèĭ òðĭ ĭ ĭ Ûä ĭ ĩ òĭ ÷ĭ Ûä øèòðĭ è ĭ ñäääĭ ñèó÷áéĭ Ûä äáĭ äðàòĭ ðĭ .....	7
0.3.2 Ñàĭ ĭ ñèĭ òðĭ ĭ èçèðòĭ ÷èäñy ĭ ĩ òĭ ÷ĭ Ûä øèòðĭ è ñèðyĭ áéäðĭ .....	8

## Äëää 1. Ī ĩäōĭä òáĭðèè èĭ òĭðĭ àöèè

1.1 Ýĭ ĭ òè ä èðèĭ òĭ ĩ ĩ äèè .....	10
1.2 Øáĭ ĭ ĩ ĩ ĩ äñèäy ĭ ĭ ääëü èðèĭ òĭ áĭ äèèçà .....	11
1.3 Ēĭ èäëüĭ äy ðáĭ äĭ ĭ èçàöëy .....	13
1.4 Ī ðàèòè÷äñèäy ñòĭ èéĭ ñòü .....	14

## Äëää 2. Ñòðĭèòäëüĭ Ûä áéĭèè äëy ñçääĭ èy èðèĭ òĭ ñòáĭ

2.1 Ēĭ ĭ äðóyĭ òĭ Ûä äáĭ äðàòĭ ðĭ .....	16
2.1.1 Äáĭ äðàòĭ ðĭ ĭ ñäääĭ ñèó÷áéĭ Ûò ÷èñäè .....	16
2.1.2 Ēĭ ĭ áéĭ èðĭ äáĭ èä ĒĒÄ è ĭ ðĭ äðàĭ ĭ ĭ äy ðäàèèçàöëy .....	18
2.2 Ēðèĭ òĭ áĭ äèèç èĭ ĭ äðóyĭ òĭ Ûò äáĭ äðàòĭ ðĭ ä .....	20
2.2.1 Äñèðùðèä èĭ ĭ äðóyĭ òĭ Ûò äáĭ äðàòĭ ðĭ ä (ĭ áóñä÷áĭ ĭ Ûò) .....	21
2.2.2 Óñä÷áĭ ĭ Ûä èèĭ áéĭ Ûä èĭ ĭ äðóyĭ òĭ Ûä äáĭ äðàòĭ ðĭ ñ èçääñòĭ Ûĭ è ĭ äðàĭ àððàĭ è .....	22
2.2.3 Óñä÷áĭ ĭ Ûä èèĭ áéĭ Ûä èĭ ĭ äðóyĭ òĭ Ûä äáĭ äðàòĭ ðĭ ñ ĭ áèçääñòĭ Ûĭ è ĭ äðàĭ àððàĭ è .....	24
2.3 Ðäàèñòðĭ ñäèèää .....	24
2.3.1 Äèääáðäè÷äñèèä ñáĭ èñòää ðäàèñòðĭ ä ñäèèää ñ èèĭ áéĭ ĭ é ĭ äðàòĭ ĭ é ñäyçĭĭ ..	25
2.3.2 ÐÑĒĪ Ñ ĭ äèñèĭ äëüĭ ĭ äĭ ĭ äðèĭ ää è ĭ ðèĭ èòèáĭ Ûä ĭ ĭ ĭ äĭ ÷èáĭ Û .....	27
2.3.3 Ðäàèñòðĭ Òèáĭ ĭ à÷è è Ääèòà, è èò ĭ ðĭ äðàĭ ĭ ĭ äy ðäàèèçàöëy .....	29

2.4 Í áeí òí ð ù á è ò í à è .....	33
------------------------------------	----

**Ãèààà 3. Ñòàðèñòè÷àñèèà ñâî éñòàà  
è ì áð ù ñèî æí î ñòè ì î ñèàâî ààðàè ù í ñòàé**

3.0 Í î ä ò í ä ù ê à í à è è ç ò .....	35
---	----

3.1 Ñòàðèñòè÷àñèèà ñâî éñòàà ì î ñèàâî ààðàè ù í ñòàé .....	36
---	----

3.1.1 Í î ñòóèà ò ù Ã î è î ì à à .....	36
---	----

3.1.2 Ñòàðèñòè÷àñèèà ò à ñ ò ù .....	37
--------------------------------------	----

3.1.2.1 Ò à í ð à ò è ÷ à ñ è è è ò ó í à à ì á í ò .....	37
---	----

3.1.2.2 × à ñ ò ì ò í ù é ò à ñ ò .....	38
---	----

3.1.2.3 Í î ñèàâî ààðàè ù í é ò à ñ ò .....	38
---	----

3.1.2.4 Ò à ñ ò ñ à ð è è .....	39
---------------------------------	----

3.1.2.5 À à ò î è î ð ð à è ÿ ò è î í í ù é ò à ñ ò .....	39
---	----

3.1.2.6 Ó í è à à ð ñ à è ù í ù é ò à ñ ò .....	39
---	----

3.1.2.7 Ò à ñ ò ì î ä ò í ð à í è é .....	41
---	----

3.1.2.8 Ñ ð à à í á í è à ò à ñ ò î â ì - ã ð à ì ì .....	42
---	----

3.1.2.9 Ê î ì á è í è ð î à à í è à ò à ñ ò î â .....	42
---	----

3.1.3 Í ò ñ à ÷ à í è à ñ è à à ù ò ì î ñ è à â î à à ð à è ù í î ñ ò à é .....	43
---	----

3.2 È è í á è í à ÿ ñ è î æ í î ñ ò ù ì î ñ è à â î à à ð à è ù í î ñ ò à é è ì ð à í á ð à ç î à à í è ÿ .....	43
---	----

3.2.1 Ê î í ò à í ò è ÿ è è í á è í î é ñ è î æ í î ñ ò è .....	43
---	----

3.2.2 À è à î ð è ò ì è è í á è í î â ñ è î ò à ç à Á à ð è à è à ì ì à - Ì ÿ ñ ñ è .....	44
---	----

3.2.3 Å ñ ò à ñ ò à à í í à ÿ è í ò à ð ì ð à ò à ò è ÿ à è à î ð è ò ì à Á à ð è à è à ì ì à - Ì ÿ ñ ñ è .....	47
---	----

3.2.4 Å ð ó à è à ì à ò í ä ù á í à è è ç à è è í á è í î é ñ è î æ í î ñ ò è .....	50
---	----

3.2.5 Í ð à í á ð à ç î à à í è ÿ .....	51
---	----

3.2.5.1 À è ñ è ð à ò í î à ì ð à í á ð à ç î à à í è à Ó ò ð ù à è è è í á è í à ÿ ñ è î æ í î ñ ò ù .....	51
---	----

3.2.5.2 Í ð à í á ð à ç î à à í è à Ó í è ø à è á ó è à à ù ò ó í è ø è è .....	53
---	----

3.2.5.3 Í ð à í á ð à ç î à à í è à à è à à à ð à è ÷ à ñ è î é í ì ð ì à è ù í î é ò ì ð ì ù .....	54
---	----

3.2.6 Í ð ì ò è è ù è è í á è í î é ñ è î æ í î ñ ò è .....	56
---	----

3.3 Í à ð è î à è ÷ à ñ è è à ì î ñ è à â î à à ð à è ù í î ñ ò è .....	57
---	----

3.3.1 Í ð à à ì à ò è ÷ à ñ è è à ñ ì ì á ð à è à í è ÿ .....	57
---	----

3.3.2 Ò à í ð à ò è ÷ à ñ è è è á í à è è ç ì à ð è î à è ÷ à ñ è è ò ì î ñ è à â î à à ð à è ù í î ñ ò à é .....	58
---	----

3.4 Ñ ó ì ì ù è ì ð ì è ç à à à à í è ÿ ì à ð è î à è ÷ à ñ è è ò ì î ñ è à â î à à ð à è ù í î ñ ò à é .....	59
---	----

3.4.1 Ñ ó ì ì ù ì à ð è î à è ÷ à ñ è è ò ì î ñ è à â î à à ð à è ù í î ñ ò à é .....	59
---	----

3.4.2 Í ð ì è ç à à à à í è ÿ ì à ð è î à è ÷ à ñ è è ò ì î ñ è à â î à à ð à è ù í î ñ ò à é .....	60
---	----

3.4.3 Í à ù à ÿ í è à í ÿ ð à à í è ò à à è ÿ è è í á è í î é ñ è î æ í î ñ ò è ì ð ì è ç à à à à í è ÿ .....	61
---	----



**Ãæãã 5. Êðèì òíãðàòè÷ãñèà ôóí êöèè. Êðèàððèè  
í àèèí áéí îñòè è ì àòíäû êíí ñòðóèðíãáí èÿ**

5.0 Î áùèé í áçîð .....	119
5.1 Êíððãÿöèííí úé èì ì óí èòàò ì ìðÿãèà k.....	122
5.1.1 Áãçíãúá ìíí ÿòèÿ è ðãçóèüòàòû äèÿ óçèíã áãç ì àì ÿòè .....	122
5.1.2 Êíí ñòðóèðíãáí èà êíððãÿöèííííí-èì ì óíí ùð ôóí êöèè .....	124
5.1.3 Êíððãÿöèííí úé èì ì óí èòàò è ààòí ì àò ñ ì àì ÿòüð .....	126
5.2 Êèãññèòèèàöèÿ Î àéãðà-Øàòôãäèüãðà äèÿ êðèàððèèãá í àèèí áéí îñòè .....	129
5.2.1 Ðãññòíÿí èà äí èèí áéí ùð ôóí êöèè .....	130
5.2.2 Ôóí êöèè ñ èèí áéí îñòðóèðíãáí .....	131
5.2.3 Ñíããðøáí í ùá í àèèí áéí ùá ôóí êöèè .....	131
5.3 Ááí ò-ôóí êöèè .....	132
5.3.1 Êíí ñòðóèèèÿ Î àèíðáí ù-Î àèòàððèáí äà è ááí ò-íòí áðãæáí èÿ Î þáãðã .....	133
5.3.2 Êíí ñòðóèèèè Êãðèã .....	134
5.3.3 Î áùãÿ êíí ñòðóèèèÿ Äíãããððèí à .....	137
5.4 Êðèàððèèè ðãñí ðí ñòðáí áí èÿ è ÿèãñòè÷í ùá ôóí êöèè .....	141
5.4.1 Ñòðíãèè èããèí í úé êðèàððèèè è êðèàððèèè ðãñí ðí ñòðáí áí èÿ .....	141
5.4.2 Êíí ñòðóèðíãáí èà áóèããúð ôóí êöèè, óáí àéãòáí ðÿðùèò êðèàððèèÿí ñããèáí ñèðíãáí í îñòè, í àèèí áéí îñòè è ðãñí ðí ñòðáí áí èÿ .....	142
5.4.2.1 Áãçíãúá ìíí ÿòèÿ è àìí ìãðàò áãàì ððíãúð ì àòðèò.....	142
5.4.2.2 Êíí íèòáí àòèÿ è ðãñùáí èáí èà ìíñèããíããòãèüí ì ñòãé.....	145
5.4.2.3 Î ìãèòèèãòèÿ è ìãðáí ìíãæáí èà ìíñèããíããòãèüí ì ñòãé.....	147
5.4.2.4 Áùñí êíí í àèèí áéí ùá ñããèáí ñèðíãáí í ùá ôóí êöèè, óáí àéãòáí ðÿðùèà êðèàððèèð ðãñí ðí ñòðáí áí èÿ áí èüøí é ñòáí áí è.....	149
5.4.3 Ýèãñòè÷í ùá ôóí êöèè .....	150
5.4.3.1 Ñíãí èñòãã ÿèãñòè÷í ùð ôóí êöèè .....	150
5.4.3.2 Êíí ñòðóèðíãáí èà ìíãúð ÿèãñòè÷í ùð ôóí êöèè èç óæã èçããñòí ùð .....	151
5.4.3.3 Î ðáíããçíãáí èà èèí áéí ùð ÿèãñòè÷í ùð ôóí êöèè á í àèèí áéí ùá .....	152
5.5 Ðãèí ì áí ààòèè êíí ñòðóèòíðáí êðèè òí ñòáí .....	153

## **Ãæàà 6. Ñõàì ù ñ í àðààí îì áðí ùì äâèæáí èàì ðããèñòðíâ è áàç ì àì yòè**

6.0 Í àðààí îì áðí ùì äâèæáí èà èàè ñì ì ñì á äì ñòèæáí èy í æèì áéí î ñòè .....	154
6.1 Î áùèè í áçí ð èí í ñòðóèöèè ñ í àðààí îì áðí ùì äâèæáí èàì ðããèñòðíâ .....	155
6.1.1 Ñõàì ù ñ óì ðããèyðùèì ðããèñòðíì , èð ì áðèì ä è èèì áéí äy ñèì æí î ñòù .....	155
6.1.1.1 Áàçí àäy ñõàì à , äáí àðàòì ðù "ñòì ì -äì àðàä" è "ì äèì -ääà øääà" .....	155
6.1.1.2 Î áðèì ä è èèì áéí äy ñèì æí î ñòù .....	156
6.1.1.3 Ááí àðàòì ð ñ ì àðàì àæàðùèè ñy øääì ì .....	158
6.1.1.4 Êãñèääí ùé äáí àðàòì ð .....	159
6.1.1.5 Ñæèì àðùèé äáí àðàòì ð .....	160
6.1.2 Ñõàì ù ñ ñàì í óì ðããèáí èàì .....	161
6.1.2.1 Ááí àðàòì ð [d,k]-ñàì í óñà-áí èy .....	161
6.1.2.2 Ñàì í ñæèì àðùèé äáí àðàòì ð .....	162
6.2 Êãñèääí ùà äáí àðàòì ðù .....	163
6.2.1 Êðèì òì äðàòè-ãñèèà ñàì èñòàà "øää <sub>k,m</sub> " -èãñèääì á .....	164
6.2.2 Êðèì òì àì àèç èãñèääì á .....	166
6.2.3 Ñèñòàì àðè-ãñèèäy àðàèà Î áí èèì +-è .....	169
6.3 Ñæèì àðùèé è ñàì í ñæèì àðùèé äáí àðàòì ðù .....	173
6.3.1 Ñæèì àðùèé äáí àðàòì ð .....	173
6.3.1.1 Êì í ñòðóèöèèy , ì áðèì ä , èèì áéí äy ñèì æí î ñòù è ñòàòèñòè-ãñèèà ñàì èñòàà .....	173
6.3.1.2 Î ðèèì æáí èà ì ðáì áðàçí ááí èy Óóðüà è ε-ñì áùáí í ùð ðãñì ðããèáí èè á áí àèçà ðããèñòðíâ ñ ì àðàì áí í ùì è òì -èàì è ñúàì à è ÑÃ .....	175
6.3.1.3 Êðèì òì áí àèòè-ãñèèà ì ì äòì äù è ãñèðùòèð ñõàì ù .....	178
6.3.1.4 Áñì àèòù àì ì àðàòì í é è ì ðì áðàì ì í í é ðããèçàòèè .....	179
6.3.2 Ñæèì àðùèé Ôèáí í à +-è-ääí àðàòì ð (Fish) è äáì ãñèðùòèà .....	180
6.3.2.1 Î áí áùáí í ùé ñæèì àðùèé äáí àðàòì ð è àèáì ðèòì Fish .....	180
6.3.2.2 Áñèðùòèà èðèì òì ñõàì ù Fish .....	181
6.3.3 Ñàì í ñæèì àðùèé äáí àðàòì ð .....	184
6.3.3.1 Ñæàòèà è ñàì í ñæàòèà .....	185
6.3.3.2 Î áðèì ä è èèì áéí äy ñèì æí î ñòù , ì ðèì áðù è yèñì áðèì áí òàèüí ùà ðãçóèüòàòù .....	185

6.3.3.3 Êðèì òì áì àèèç .....	187
6.4 Æñèðùðèà ñòàì ñ í àðááí îì àðí ùì äàèæáí èàì .....	190
6.4.1 Êðàòèèé í áçì ð î ñí î áí ùð ðáçóèùòàðì á .....	190
6.4.2 Æî ñòàì î áèáí èà í à÷-àèüí î áì çàì î éí áí èý ðáæñòðà í à î ñí î áá í î áì é ì àðù ðàññòì ýí èý ì áæáó î î ñèááí áàðàèüí î ñòýì è .....	192
6.4.3 Àðàèà ãñòðàèèááí èàì è ááðí ýòí î ñòí àý èí ððáèýòèí í í àý àðàèà .....	196
6.4.4 Æî ñòàì î áèáí èà î î èèí î ì à í àðáòí î é ñáýçè è áùñòðáý èí ððáèýòèí í í àý àðàèà .....	200

## Æèàà 7. Ñòàì ù ñ í àì ýòùð

7.1 Î áùèé í áçì ð .....	208
7.1.1 Ñòàì ù ñ ðááí îì àðí ùì äàèæáí èàì è í àì ýòùð .....	208
7.1.2 Ñòàì ù í à ðáæñòðàð ñáæèà ñ î ì àðàòèáé î áðáí î ñà .....	209
7.1.3 Ñòàì ù ñ í àðááí îì àðí ùì äàèæáí èàì è í àì ýòùð .....	212
7.2 Êí ððáèýòèí í í ùà ñáí èñòàà èí ì áèí èðòðùèò óçèí á ñ 1 áèòì ì í àì ýòè .....	213
7.2.1 Ááçì ááý ñòàì à ñòí ì àòí ðà .....	213
7.2.2 Î áí áùáí í úé èí ì áèí èðòðùèé óçáé ñ 1 áèòì ì í àì ýòè .....	214
7.2.3 Êí ððáèýòèý, î áóñèí áèáí í àý èçááñòí ùì áùòí áí ì .....	216
7.2.4 Êðèì òì áì àèèç ñòí ì àòí ðà ñ ááóí ý áðí áàì è .....	217
7.3 Êí ì áèí èðòðùèé óçáé ñ î ðí èçáí èüí ùì ÷-èñèí ì áèò ì àì ýòè .....	219
7.3.1 Î áí áùáí í úé ááí è÷ í úé èí ì áèí èðòðùèé óçáé ñ í àì ýòùð è èí ððáèýòèí í í ùà ñáí èñòàà ááèòì ðí ùð áóèááùð òóí èòèé .....	219
7.3.2 Êí ððáèýòèí í í ùà ñáí èñòàà èí ì áèí èðòðùèò óçèí á ñ í àì ýòùð .....	222
7.3.3 Ì áòí á áí ì ðí èñèí áòèè èèí áéí î é î î ñèááí áàðàèüí î é ñòàì î é .....	224
7.3.4 Êí ððáèýòèí í í àý àðàèà .....	227
7.4 Ðáæñòðù ñáæèà ñ î áðáí î ñí ì è 2-áàè÷-áñèèé áí àèèç .....	228
7.4.1 Î áçì ð 2-áàè÷-áñèèé ÷-èñáè .....	229
7.4.2 Ðáæñòðù ñáæèà ñ í àì ýòùð, èð ðáæèèçáòèý, ððááí ááí èý é í àì ýòè .....	230
7.4.3 Áí àèèç ÐÑÌ ÑÌ .....	232
7.4.4 2-áàè÷-áñèèé ðáçì áò è ñèí æí î ñòù .....	235
7.4.5 Æèáí ðèòì ðáòèí í àèüí î é áí ì ðí èñèí áòèè .....	237
7.4.6 2-áàè÷-áñèèé èðèì òì áì àèèç ñòí ì àòí ðà .....	239
7.4.7 Æèèí í ùà î î ñèááí áàðàèüí î ñòè è èð ñòàðèñòè÷-áñèèà ñáí èñòàà .....	240
7.4.8 ÐÑÌ ÑÌ ì áèñèí àèüí î áí ì àðèí áà è èðèì òì ñòàì ù í à èð î ñí î áá .....	241

## **Àèààà 8. Êîí êðàòí ùà ñòàì ù êðèì òíàáí àðàòíðíà è ñàì íñèì òðíí èçèðóðùèàñŷ øèòðù**

8.1 Í áçíð ðàí í èò ñòàì .....	245
8.1.1 Ááí àðàòíð ÁáÒÒà .....	245
8.1.2 Ááí àðàòíð Í èáññà .....	246
8.1.3 Ááí àðàòíð-ì óèùòèì èáññí ð Áæáí í èì ãñà .....	247
8.1.4 Í í ðíáí áùé ááí àðàòíð .....	248
8.1.5 Ááí àðàòíð ñèàèŷðí í áí í àðàì í íæáí èŷ .....	249
8.1.6 Ááí àðàòíð Áí èüòðàì à .....	250
8.1.7 Ááí àðàòíð "1/p" .....	251
8.1.8 Ááí àðàòíð ñóì ì èðí ááí èŷ .....	253
8.1.9 Ðáí óááùé ááí àðàòíð .....	254
8.1.10 Áäèòèáí ùé ááí àðàòíð .....	255
8.1.11 Ááí àðàòíð ÁèÒÒíðàà .....	256
8.2 Àèãíðèòì Á5 .....	257
8.2.1 Í í èñáí èà êðèì òí ñòàì ù .....	257
8.2.2 Êðèì òí áí àèèç øèòðà .....	259
8.3 Àèãíðèòì RC4 .....	260
8.3.1 Í í èñáí èà êðèì òí ñòàì ù .....	260
8.3.2 Êðèì òí áí àèèç .....	262
8.4 Àèãíðèòì SEAL .....	263
8.4.1 Ñàì àéñòáí í ñáááí ñèó-àéí ùò òóí èòèé .....	263
8.4.2 Í ñí ááí í í ñòè SEAL .....	264
8.4.3 Í í èñáí èà àèãíðèòì à .....	265
8.4.4 Ñòí ééí ñòü SEAL .....	268
8.5 Í áçíð êðèì òí ñòàì 1990-ò áí áí à .....	268
8.5.1 Õèèüòð-ááí àðàòíð í à í ñí í áá àèãíðèòì à ñæàðèŷ ááí í ùò Çèàà-Èàì í áèà .....	268
8.5.2 Í í àèòèòèðí ááí í ùé èèì áéí ùé èí í áðóŷí òí ùé ááí àðàòíð (×àì ááðñà) .....	271
8.5.3 Èáñèàà ñ í áðááí í ì áðí ùì ááèæáí èàì (×àì ááðñà) .....	273
8.5.4 Àèãíðèòì WAKE .....	275
8.5.5 Àèãíðèòì PIKE .....	276
8.5.6 Àèãíðèòì GOAL .....	277
8.5.7 Àèãíðèòì ORYX .....	278
8.5.8 Ááí àðàòíð ISAAC .....	280
8.5.9 Chameleon - í í áí à í ðèèí æáí èà êðèì òí áðàòèè .....	283

8.6 Nài îñèi òðî í èçèðòþùèàñý øèòðû .....	284
8.6.1 Êî í òáî òóàèüí àý ñòáì à .....	285
8.6.2 Ðàèóðñèáí àý àððèòàèóóðà Ì àóðàðà .....	286
8.6.3 Ñòáì à Äýì áí à í à ðáàèñòðà ñáàèàà ñ òñèí áí ùì äîíîèí áí èàì .....	287

## Ãèàà 9. Í îâûá ì àòîäû êðèòîìáí àèèçà

9.1 Ì àòî ä "ãñòðà+à ì îñáðáàèí á" .....	290
9.2 Êðèòîì áðàòè+ãñèà ñèááí ñòè ðáñèí òðî í èçàòèè .....	291
9.2.1 Òèí ù ðáñèí òðî í èçàòèè è èó èí òáðî ðàòàòèý .....	292
9.2.2 Ì áùàý àòàèà í àèèí áéí î èèüòðóáì ùò ñèñòáì .....	294
9.2.3 Àòàèà ì óèüòè èáèñî ð-ááí áðàòî ðà .....	296
9.3 Äèòóáðáí òèàèüí ùé êðèòîìáí àèèç .....	297
9.3.1 Äáàèòèáí ùé ãñòáñòááí í ùé ì îðî +í ùé øèòð .....	297
9.3.2 Äèòóáðáí òèàèüí àý àòàèà .....	298
9.3.3 Òáí ðàòè+ãñèè ááçèñ àòàèè .....	299
9.4 Èèí áéí ùé êðèòîìáí àèèç .....	300
9.4.1 Èèí áéí ùá ì îáàèè ì îðî +í ùò øèòðî á .....	300
9.4.2 Èèí áéí ùé àì àèèç ñáí áðàòî ðî á í à ì ñí í áà ðáàèñòðî á ñáàèà .....	302
9.5 Ì àòî äû àèñèðáòîì é ì ì òèè èçàòèè: ñèì óèýòî ð ì ðæèà è ááí àòè+ãñèè àèá ðèòì .....	302
9.5.1 Ñèì óèýòî ð ì ðæèà è àèá ðèòì Ì àòðî ì èèà .....	302
9.5.2 Êî ððáèýòèí í àý àòàèà, ì ì àèòèèèðî ááí í àý ñèì óèýòî ð ì ì ðæèà .....	305
9.5.3 Ááí àòè+ãñèè àèá ðèòì ù .....	306
9.6 Ì ì òèè èçàòèè òì àèèí îáî ì áðááí ðà èèþ+áé .....	307
9.7 Ì ñóòáñòáí ááí èè ñòì èèèò ðáàèñòðî á ñáàèà .....	310
9.7.1 Êî í òáî òóàèüí àý ì îáàèè .....	310
9.7.2 Ì ì ðáààèáí èý .....	311
9.7.3 Ñóòáñòáí ááí èà ñòì èèèò ÐÑÌ Ñ .....	313
9.7.4 Àòàèè èèí áéí îáî ñèí òáçà .....	315

## Ãëàà 10. Åëüòàđí àòèái úà êíí ñòđóêöèè

10.0 Åçäëÿäü í à òái ðèþ ñòí ééí ñòè .....	317
10.1 Ĩ í äöí ä ñ í í çèöèé òái ðèè ñéí æí í ñòè .....	319
10.1.1 Åaçí áúà èääè è êíí öái öèè .....	320
10.1.2 Āái áðàòí ðû .....	322
10.1.2.1 Ĩ ñááái ñéó÷àéí úé áái áðàòí ð Øài èðà .....	322
10.1.2.2 Āái áðàòí ð Áèþí à-Ĩ èèäèè .....	324
10.1.2.3 Āái áðàòí ðû RSA .....	326
10.1.2.4 Āái áðàòí ð éâääðàðè÷í úõ áú÷àòí á .....	327
10.2 Ðái áíí èçèđí áái í úá øèòðû .....	329
10.2.1 Øèòð Äèòòè .....	330
10.2.2 Øèòð "Ðèí áái Áéí éëü" .....	330
10.2.3 Øèòð Ĩ àòðáðà .....	332
10.3 Öài òè÷añèèá øèòðû .....	333
10.4 Ñèñòái à áái í èđí áái èÿ POTP .....	334

## Ãëàà ì ñèáái ÿÿ. Çàèèþ÷ái èà

I. Ñí áðái áí í äÿ ñèóòàöèÿ á í òèðûòí é èðèí òí áðàòèè .....	337
II. Êðèòàðèè äëÿ ñðáái áí èÿ àèái ðèòí í á .....	338
III. Ĩ ðí áðái í í úá è áí í áðàòí úá øèòðû .....	338
IV. Ðàçàèòèá òái ðèè .....	339
V. Æèçí ü á ðààëüí í ñ í èðà .....	339

Áèáèèíãðàòèÿ ..... 341

Áí äèí-ðóññèèé ì ðáái àòí úé óèàçàòáëü ..... 369

Ðóññèè-ái äèèéñèèé ì ðáái àòí úé óèàçàòáëü ..... 378