Áðþñ Øíàéåð

Ïðèêëàäíàÿ êðèïòîãðàôèÿ

2-å èçäàíèå

Ïðîòîêîëû, àëãîðèòìû è ñõåìû òåêñòû íà ÿçûêå Ñ

ÑÎÄÅÐÆÀÍÈÅ

Ãëàâà 3
Îñíîâíûå ïðîòîêîëû

3.1 Îáìåí êëþ÷àìè
3.2 Óäîñòîâåðåíèå ïîäëèííîñòè
3.3 Óäîñòîâåðåíèå ïîäëèííîñòè è îáìåí êëþ÷àìè
3.4 Ôîðìàëüíûé àíàëèç ïðîòîêîëîâ ïðîâåðêè ïîäëèííîñòè è îáìåíà êëþ÷àìè
3.5 Êðèïòîãðàôèÿ ñ íåñèìåòðè÷íûì êëþ÷îì
3.6 Ðàçäåëåíèå ñåêðåòà
3.7 Ñîâìåñòíîå èñïîëüçîâàíèå ñåêðåòà
3.8 Êðèïòîãðàô÷åñêàÿ çàùèòà áàç äàííûõ

Ãëàâà 4
Ïðîìåæóòî÷íûå ïðîòîêîëû

4.1 Ñëóæáû ìåòîê âðåìåíè
4.2 Ïîäñîçíàòåëüíûé êàíàë
4.3 Íåòðèâèàëüíûå öèôðîâûå ïîäïèñè
4.4 Ïîäïèñè óïîëíîì÷åííîãî ñâèäåòåëÿ
4.5 Ïîäïèñè ïî äîâåðåííîñòè
4.6 Ãðóïïîâûå ïîäïèñè
4.7 Ïîäïèñè ñ îáíàðóæåíèåì ïîääåëêè
4.8 Âû÷èñëåíèÿ ñ çàøèôðîâàííûìè äàííûìè
4.9 Âðó÷åíèå áèòîâ
4.10 Ïîäáðàñûâàíèå "÷åñòíîé" ìîíåòû
4.11 Ìûñëåííûé ïîêåð
4.12 Îäíîíàïðàâëåííûå ñóììàòîðû
4.13 Ðàñêðûòèå ñåêðåòîâ "âñå èëè íè÷åãî"
4.14 Óñëîâíîå âðó÷åíèå êëþ÷åé

Ãëàâà 5
Ðàçâèòûå ïðîòîêîëû

5.1 Äîêàçàòåëüñòâà ñ íóëåâûì çíàíèåì
5.2 Èñïîëüçîâàíèå äîêàçàòåëüñòâà ñ íóëåâûì çíàíèåì äëÿ èäåíòèôèêàöèè
5.3 Ñëåïûå ïîäïèñè
5.4 Ëè÷íîñòíàÿ êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè
5.5 Ðàññåÿííàÿ ïåðåäà÷à
5.6 Ðàññåÿííûå ïîäïèñè
5.7 Îäíîâðåìåííàÿ ïîäïèñü êîíòðàêòà
5.8 Ýëåêòðîííàÿ ïî÷òà ñ ïîäòâåðæäåíèåì
5.9 Îäíîâðåìåííûé îáìåí ñåêðåòàìè

Ãëàâà 6
Ýçîòåðè÷åñêèå ïðîòîêîëû

6.1 Áåçîïàñíûå âûáîðû
6.2 Áåçîïàñíûå âû÷èñëåíèÿ ñ íåñêîëüêèìè ó÷àñòíèêàìè
6.3 Àíîíèìíàÿ øèðîêîâåùàòåëüíàÿ ïåðåäà÷à ñîîáùåíèé
6.4 Ýëåêòðîííûå íàëè÷íûå

×àñòü II Êðèïòîãðàôè÷åñêèå ìåòîäû

Ãëàâà 7
Äëèíà êëþ÷à

Ãëàâà 8
Óïðàâëåíèå êëþ÷àìè

Ãëàâà 9
Òèïû àëãîðèòìîâ è êðèïòîãðàôè÷åñêèå ðåæèìû

Ãëàâà 10 (Òåêñò ãëàâû íà àíãëèéñêîì, sorry. Ïåðåâîä÷èê, ïîõîæå, óñòàë :-)
Èñïîëüçîâàíèå àëãîðèòìîâ

×àñòü III Êðèïòîãðàôè÷åñêèå àëãîðèòìû

Ãëàâà 11
Ìàòåìàòè÷åñêèå îñíîâû

Ãëàâà 12
Ñòàíäàðò øèôðîâàíèÿ äàííûõ DES

Ãëàâà 13
Äðóãèå áëî÷íûå øèôðû

Ãëàâà 14
È åùå îáëî÷íûõ øèôðàõ

14.1 ÃÎÑÒ
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 Äðóãèå áëî÷íûå àëãîðèòìû
14.10 Òåîðèÿ ïðîåêòèðîâàíèÿ áëî÷íîãî øèôðà
14.11 Èñïîëüçîâàíèå îäíîíàïðàâëåííûõ õýø-ôóíêöèé
14.12 Âûáîð áëî÷íîãî àëãîðèòìà

Ãëàâà 15
Îáúåäèíåíèå áëî÷íûõ øèôðîâ

15.1 Äâîéíîå øèôðîâàíèå
15.2 Òðîéíîå øèôðîâàíèå
15.3 Óäâîåíèå äëèíû áëîêà
15.4 Äðóãèå ñõåìû ìíîãîêðàòíîãî øèôðîâàíèÿ
15.5 Óìåíüøåíèå äëèíû êëþ÷à â CDMF
15.6 Îòáåëèâàíèå
15.7 Ìíîãîêðàòíîå ïîñëåäîâàòåëüíîå èñïîëüçîâàíèå áëî÷íûõ àëãîðèòìîâ
15.8 Îáúåäèíåíèå íåñêîëüêèõ áëî÷íûõ àëãîðèòìîâ

Ãëàâà 16
Ãåíåðàòîðû ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé è ïîòîêîâûå øèôðû

16.1 Ëèíåéíûå êîíãðóýíòíûå ãåíåðàòîðû
16.2 Ñäâèãîâûå ðåãèñòðû ñ ëèíåéíîé îáðàòíîé ñâÿçüþ
16.3 Ïðîåêòèðîâàíèå è àíàëèç ïîòîêîâûõ øèôðîâ
16.4 Ïîòîêîâûå øèôðû íà áàçå LFSR
16.5 A5
16.6 Hughes XPD/KPD
16.7 Nanoteq
16.8 Rambutan
16.9 Àääèòèâíûå ãåíåðàòîðû
16.10 Gifford
16.11 Àëãîðèòì M
16.12 PKZIP

Ãëàâà 17
Äðóãèå ïîòîêîâûå øèôðû è ãåíåðàòîðû íàñòîÿùèõ ñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé

17.1 RC4
17.2 SEAL

Ãëàâà 18
Îäíîíàïðàâëåííûå õýø-ôóíêöèè

Ãëàâà 19
Àëãîðèòìû ñ îòêðûòûì êëþ÷àìè

Ãëàâà 20
Àëãîðèòìû öèôðîâîé ïîäïèñè ñ îòêðûòûì êëþ÷îì

Ãëàâà 21
Ñõåìû èäåíòèôèêàöèè

Ãëàâà 22
Àëãîðèòìû îáìåíà êëþ÷àìè

Ãëàâà 23
Ñïåöèàëüíûå àëãîðèòìû äëÿ ïðîòîêîëîâ

×àñòü IV Ðåàëüíûé ìèð

Ãëàâà 24
Ïðèìåðû ðåàëèçàöèé

Ãëàâà 25
Ïîëèòèêà

Ìýòò Áëåéç. Ïîñëåñëîâèå

×àñòü V Èñõîäíûå êîäû

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

Áèáëèîãðàôèÿ