Áðþñ Øíàéåð Ïðèêëàäíàÿ êðèïòîãðàôèÿ

2-å èçäàíèå

Ïðîòîêîëû, àëãîðèòìû è èñõîäíûå òåêñòû íà ÿçûêå Ñ

ÑÎÄÅÐÆÀÍÈÅ

Óèòôèëä Äèôôè. Ïðåäèñëîâèå

Ââåäåíèå

Ãëàâà 1

Îñíîâíûå ïîíÿòèÿ

1.1 Òåðìèíîëîãèÿ 1.2 Ñòåãàíîãðàôèÿ

1.3 Ïîäñòàíîâî÷íûå è ïåðåñòàíîâî÷íûå øèôðû 1.4 Ïðîñòîå XOR

1.5 Îäíîðàçîâûå áëîêíîòû 1.6 Êîìïüþòåðíûå àëãîðèòìû 1.7 Áîëüøèå ÷èñëà

×àñòü I Êðèïòîãðàôè÷åñêèå ïðîòîêîëû

Ãëàâà 2

Ýëåìåíòû ïðîòîêîëîâ

2.1 Ââåäåíèå â ïðîòîêîëû

2.2 Ïåðåäà÷à èíôîðìàöèè ñ èñïîëüçîâàíèåì ñèììåòðè÷íîé êðèïòîãðàôèè 2.3 Îäíîíàïðàâëåííûå ôóíêöèè

2.4 Îäíîíàïðàâëåííûå õýø-ôóíêöèè

2.5 Ïåðåäà÷à èíôîðìàöèè ñ èñïîëüçîâàíèåì êðèïòîãðàôèè ñ îòêðûòûìè êë þ÷àìè 2.6 Öèôðîâûå ïîäïèñè

2.7 Öèôðîâûå ïîäïèñè è øèôðîâàíèå

2.8. Ãåíåðàöèÿ ñëó÷àéíûõ è ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé

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 íåñêîëüêèìè îòêðûòûìè êëþ÷àìè

3.6 Ðàçäåëåíèå ñåêðåòà

3.7 Ñîâìåñòíîå èñïîëüçîâàíèå ñåêðåòà

3.8 Êðèïòîãðàôè÷åñêàÿ çàùèòà áàç äàííûõ

Ãëàâà 4

Ïðîìåæóòî÷íûå ïðîòîêîëû

4.1 Ñëóæáû ìåòîê âðåìåíè 4.2 Ïîäñîçíàòåëüíûé êàíàë

4.3 Íåîòðèöàåìûå öèôðîâûå ïîäïèñè 4.4 Ïîäïèñè óïîëíîìî÷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