«Ýíèãìà» â íîâîì èñïîëíåíèè

Äèñêîâûé øèôðàòîð Â«ÝíèãìàÂ» îòëè÷àåò ïðîñòîòà êîíñòðóêöèè, âûñîêàÿ íàä¸æíîñòü ðàáîòû è îòëè÷íàÿ ñòîéêîñòü øðèôòà. Ïåð
ìèðîâîé âîéíû. Ïî êîíñòðóêöèè Â«ÝíèãìàÂ» êëàññèêè÷åñêèé êàê äëñêîâûé øèôðàòîð, îñíîâûâàþùèéñÿ íàëè÷èå
èñïîëüçîâàëè òðè ñòåïåíåíûõ ìåæäó ñîáîé øèôðîâàëüíûõ äèñêà, ñîâåðøåíñòâîâàëè, ïîâîíî ñ
ðàáîòû íàä ñîâåðøåíñòâîâàíèåì Â«ÝíèãìûÂ» íå ïðåêðàùàëèñü íè íà ìèíóòó. Ðåçóëüòàòîì òàêîãî òðóäà ñòàëî øèôðîâàëüíîå óñòðîé
Ñòîéêîñòü òàêîãî øèôðà îêàçàëàñü íå ïî çóáàì äàæå ïåðâûì à ìèðå ýëåêòðîííûì âû÷èñëèòåëÿì Colossus, ïîñòðîåííûì â ÀíãëèÈ. Ó
ïîäîáíûå áóìàãè õðàíÿòñÿ ïîä ãðèôîì Â«ÑîâåðøåííîÂ» ëèáî áûëè óíè÷òîæåíû íåìöàìè åù¸ äî êàïèòóëÿöèè Ãåðìàíèè. Ïî ðàç
ñèìâîëîâ àëôàâèòà óäîáíåå ñ÷èòàòü ðàâíûì 256, ïî ÷èñëó ðàçëè÷íûõ çíà÷åíèé áàéòà. ×èñëî äëñêîâ îáîçíà÷èì êàê n=11. Êàæäîì
Tab[i]=Tab[i][j], j=0..255, i=0..n-1 ÷èñëå 0..255, ñêëåéíàÿ â êîëüöî. Ïóñòü ïîëîæåíèå òåêóùåãî íà÷àëà êàæäîé òàáëèöû îðåàëèç
i=0..n-1. Ñ ó÷åòîì óêàçàííûõ îáîçíà÷åíèé øàã çàøèôðîâûâàíèÿ ñèìâîëà Ì äëÿ Â«ÝíèãìûÂ» ñ ðåãóëÿðíûì äâèæåíèåì øèôðîâàëüíûõ
âû÷èñëÿåì n ðàç: Â Â Â a.Â Â Â Â Â Â M = Tab[i, M]; Â Â Â b.Â Â Â Â Â Â i = i + 1; Â Â Â c.Â Â Â Â Â Â Êîíåö öèêëà i; 3.Â Â
Â Â Â a.Â Â Â Â Â Â Ptr[i] = (Ptr[i]+k) mod256; Â Â Â b.Â Â Â Â Â Åñëè k=0, óõîäèì íà 4.e.; Â Â Â c.Â Â Â Â Â Â Åñëè Ptr[i]=
e.Â Â Â Â Â Â i=i+1; Â Â Â f.Â Â Â Â Â Â Êîíåö öèêëà i. Õàíòè÷åñêè äâèæåíèå øèôðîâàëüíûõ äiñêîâ ìîäåëèðóåòñÿ ñëåäóþ
a.Â Â Â Â Â Â M = Tab[i, M]; b.Â Â Â Â Â i = i + 1; c.Â Â Â Â Â Â Êîíåö öèêëà i; 3.Â Â Â Â Â Ïóñòü k=1; 4.Â Â Â Â Â Â öèêë
(Ptr[i]*i+1) mod256; b.Â Â Â Â Â i=i+1; c.Â Â Â Â Â Â Êîíåö öèêëà i. Âñÿ íåðåãóëÿðíîñòü çäåñü ìîäåëèðóåòñÿ ñòðîêîé 4.à,
ñèìâîëà. Îáíàêî ýòî íå ïðèíåñ¸ò ïðàêòè÷åñêè íèêàêèõ ïðåèìóùåñòâ. Îáðàòèìîñòü ïîëíàíîãî øèôðóþùèõ ïðåîáðàçîâàíèé íå âûçûâà
ïðîòèâîïîëîæíûé è çàìåíà òàêèõ èíâåðñíûìè èì InvTab[i],i=0..n-1 ñ èñïîëüçîâàíèåì ñîîòíîøåíèÿ InvTab[i,Tab[i,j]]=j,j=0..255,i=0..n-1. Ó
òî ïðîùåññ çàøèôðîâàíèÿ ìîæíî ïîñòðîèòü è íà óïðàâëåíèè ïðÿäêîì ïðîõîæäåíèÿ ñèìâîëîâ ÷åðåç ñèñòåìó òàáëëö. Ïðàâäà, îíà ñîîòâå
èç ðàñ÷îòðåííûõ ðàíåå. Íî äåëàòü ýòîãî ìû íå áóäåì, à ïðîñòî ñêàæåì, ÷òî Â«ÝíèãìàÂ» ïîäîáíîé êîíñòðóêöèè ìîæåò áûòü ðåàëèçîâà
1 è óêàçàòåëé Ptr[i], i=0..n-1 ê íèì. Â ýòîì ñëó÷àå ïðèíÿòí àëãîðèòì, ÷àñòè÷íî ïîçàèìñòâîâàííûé èç ïîëíàíèÿ øèôðà RC4 Ðîíà Ðèâ
Tab[0,i]=i,i=0..255. Çàòåì åå ýëåìåíòû ïåðåñòàâëÿåì â ñîîòâåòñòâèè ñî çíà÷åíèåì êëþ÷à, öèêëè÷åñêè ïîâòîðÿÿ ïî ìåðå íåîáõîäèìîñ
ïðîöåññ ðàíäîìèçàöèè òàáëöû Tab[0], îñóùåñòâëÿåìûé ñëåäóþùèì îáðàçîì. 1.Â Â Â Â Â Ïóñòü i=0; 2.Â Â Â Â Â Â öèêëå ñî ñ
Tab[0, Tab[0,i]]) mod256; b.Â Â Â Â Â Ìåíÿåì ìåñòàìè ýëåìåíòû Tab[0,i] è Tab[0,j]; c.Â Â Â Â Â Â i = i + 1; d.Â Â Â Â Â Â Êîíåö öè
Tab[i],i=1..n ïîëó÷åííûì ïðèìåíåíèåì ïîëíàíîé ïðîöåäóðû ê ïðåäûäóùåé òàáëèöå. Íà÷àëüíûå çíà÷åíèÿ óêàçàòåëåé Ptr[i], i=0..n-1 â
ñ÷åò÷èêîì i âû÷èñëÿì n ðàç: Â Â Â a.Â Â Â Â Â Â Ptr[i] = (Tab[i, 0] + Tab[i, Tab[i,0]]) mod256 èëè Ptr[i] = Â Â Â = (Tab[i, 0] +
mod n; Â Â Â b.Â Â Â Â Â i = i + 1; Â Â Â c.Â Â Â Â Â Â Êîíåö öèêëà i. Çäåñü çà íåèìåíåì ëó÷øåãî îïòü-òàêè èñïîëüçîâàíî
ïîñòîÿííîâî ðàñïàéêè êîíòàêòîâ Â«ÝíèãìûÂ» âëå÷åò ðåãóëÿðíóþ â êëàññè÷åñêîì èëè íåðåãóëÿðíóþ â óñîâåðøåíñòâàííûõ íåðà
øèôðó RC4. Ïðàâäà, ïîñëåäíå ñîîòâåòñòâóåò ðåàëüíî íåîñóùåñòâèìîé ïðåðàñïàéêå äèñêîâ Â«ÝíèãìûÂ» íåïîñðåäñòâåííî â õîäå