# Âûñîêîóðîâíåâûå ìåòîäû èíôîðìàòèêè è ïðîãðàììèðîâàíèÿ

Ââåäåíèå

Âîîáùå, èñòîðèþ êðèïòîãðàôèè ìîæíî ñ÷èòàòü ðàâíîé ïî âîçðàñòó èñòîðèè ñóùåñòâîâàíèÿ ïèñüìåííîñòè, ïîòîìó ÷òî èìåííî ñ ïîÿâëåíèåì ïèñüìåííîñòè âîçíèêëà ïîòðåáíîñòü ïðèäóìûâàòü ðàçëè÷íûå ñïîñîáû äëÿ õðàíåíèÿ èíôîðìàöèè â âèäå, äîñòóïíîì òîëüêî äëÿ îïðåäåëåííîãî êðóãà ëèö. Íàïðèìåð, äî íàøåé ýðû áûë ïðèäóìàí èçâåñòíûé «Øèôð Öåçàðÿ», êîòîðûé çàêëþ÷àëñÿ â çàìåíå êàæäîãî ñèìâîëà â òåêñòå íà ýëåìåíò, îòñòîÿùèé îò íåãî â àëôàâèòå íà ôèêñèðîâàííîå ÷èñëî ïîçèöèé.

Åñòåñòâåííî, ÷òî ëþäè, îò êîòîðûõ èíôîðìàöèÿ óòàèâàëàñü, èñêàëè âñÿ÷åñêèå ñïîñîáû ðàñøèôðîâàòü çàêîäèðîâàííûå ñîîáùåíèÿ. Òàêèõ ëþäåé ñåé÷àñ íàçûâàþò êðèïòîàíàëèòèêàìè. Îáå âðàæäóþùèå ñòîðîíû íàõîäèëèñü â ïîñòîÿííîì ïðîòèâîáîðñòâå: ïåðâûå ïîñòîÿííî ïðèäóìûâàëè íîâûå øèôðû, ñ ïåðâîãî âçãëÿäà íåäîñòóïíûå äëÿ êðèïòîàíàëèòèêîâ, à âòîðûå íàõîäèëè ñïîñîáû äåøèôðîâêè ñêðûòûõ ñîîáùåíèé.

Áëàãîäàðÿ ðàáîòå Àáó àëü - Êèíäè îêàçàëîñü, ÷òî øèôðû òèïà «Øèôðà Öåçàðÿ» (òî åñòü ìîíîàëôàâèòíûå øèôðû, â êîòîðûõ êàæäîé áóêâå êîäèðóåìîãî òåêñòà ñòàâèòñÿ â ñîîòâåòñòâèå îäíîçíà÷íî êàêàÿ-òî øèôðîâàííàÿ áóêâà) äîâîëüíî-òàêè ëåãêî ïîääàþòñÿ ÷àñòîòíîìó êðèïòîàíàëèçó. Âîçíèêëà ïîòðåáíîñòü â ðàçðàáîòêå òàêèõ øèôðîâ, ðó÷íàÿ ðàñøèôðîâêà êîòîðûõ ìîæåò ïîòðåáîâàòü î÷åíü çíà÷èòåëüíûõ óñèëèé. È íà ñìåíó ìîíîàëôàâèòíûì øèôðàì ïðèøëè ïîëèàëôàâèòíûå øèôðû. Àáó àëü - Êèíäè ïåðâûì ïðåäëîæèë èñïîëüçîâàòü ìíîãîàëôàâèòíûé øèôð. Â åâðîïåéñêèõ ñòðàíàõ ýòî ïðîèçîøëî â ýïîõó Âîçðîæäåíèÿ, êîãäà ðàçâèòèå òîðãîâëè ïîòðåáîâàëî íàäåæíûå ñïîñîáû çàùèòû èíôîðìàöèè. Îäíèì èç ïåðâûõ ïðåäëîæèë ïîëèàëôàâèòíûé øèôð èòàëüÿíñêèé àðõèòåêòîð Áàòèñòå Àëüáåðòè. Âïîñëåäñòâèè äàííûé øèôð ïîëó÷èë èìÿ äèïëîìàòà XVI âåêà Áëåçà äå Âèæåíåðà. Òàêæå âêëàä â ðàçâèòèå ïîëèàëôàâèòíûõ øèôðîâ âíåñ íåìåöêèé àááàò XVI âåêà Èîãàíí Òðèñåìóñ. Ïðîñòûì, íî ñòîéêèì ñïîñîáîì ïîëèàëôàâèòíîé çàìåíû ÿâëÿåòñÿ øèôð Ïëåéôåðà, îòêðûòûé â íà÷àëå XIX âåêà ×àðëüçîì Óèòñòîíîì.

Ýòîò øèôð èñïîëüçîâàëñÿ âïëîòü äî I ìèðîâîé âîéíû. Ïîñëåäíèì ñëîâîì â ðàçâèòèè ïîëèàëôàâèòíûõ øèôðîâ ñòàëè òàê íàçûâàåìûå ðîòîðíûå ìàøèíû, êîòîðûå ïîçâîëÿëè ëåãêî ñîçäàâàòü óñòîé÷èâûå ê êðèïòîàòàêàì ïîëèàëôàâèòíûå øèôðû. Ïðèìåðîì òàêîé ìàøèíû ÿâëÿåòñÿ íåìåöêàÿ ìàøèíà Enigma, ðàçðàáîòàííàÿ â 1917 ã. Ýäâàðäîì Õåáåðíîì.

Öåëüþ êóðñîâîé ðàáîòó ÿâëÿåòñÿ ðåàëèçàöèÿ êðèïòîãðàôè÷åñêîãî àëãîðèòìà øèôðîâàíèÿ è äåøèôðîâàíèÿ ñ èñïîëüçîâàíèåì øèôðà Âèæåíåðà.

1.Ïîëèàëôàâèòíûå øèôðû

Ââîäèòü ïîíÿòèå ïîëèàëôàâèòíîãî øèôðà óäîáíåå âñåãî, ñíà÷àëà îïðåäåëèâ ìîíîàëôàâèòíûé øèôð, ÷òî áûëî ñäåëàíî â èñòîðè÷åñêèõ ñâåäåíèÿõ.

Ñóòü ïîëèàëôàâèòíîãî øèôðà çàêëþ÷àåòñÿ â öèêëè÷åñêîì ïðèìåíåíèè íåñêîëüêèõ ìîíîàëôàâèòíûõ øèôðîâ ê îïðåäåë¸ííîìó ÷èñëó áóêâ øèôðóåìîãî òåêñòà. Íàïðèìåð, ïóñòü ó íàñ èìååòñÿ íåêîòîðîå ñîîáùåíèå x1 , x2 , x3 , ….. xn , …… x2n , ….., êîòîðîå íàäî çàøèôðîâàòü. Ïðè èñïîëüçîâàíèè ïîëèàëôàâèòíîãî øèôðà èìååòñÿ íåñêîëüêî ìîíîàëôàâèòíûõ øèôðîâ (íàïðèìåð, n øòóê). È â íàøåì ñëó÷àå ê ïåðâîé áóêâå ïðèìåíÿåòñÿ ïåðâûé ìîíîàëôàâèòíûé øèôð, êî âòîðîé áóêâå - âòîðîé, ê òðåòüåé - òðåòèé….. ê n-îé áóêâå - n-é, à ê n+1 îïÿòü ïåðâûé, íó è òàê äàëåå. Òàêèì îáðàçîì, ïîëó÷à¸òñÿ äîâîëüíî-òàêè ñëîæíàÿ ïîñëåäîâàòåëüíîñòü, êîòîðóþ óæå íå òàê ïðîñòî âñêðûòü, êàê îäèí ìîíîàëôàâèòíûé øèôð. Ñàìûì âàæíûì ýôôåêòîì, äîñòèãàåìûì ïðè èñïîëüçîâàíèè ïîëèàëôàâèòíîãî øèôðà, ÿâëÿåòñÿ ìàñêèðîâêà ÷àñòîò ïîÿâëåíèÿ òåõ èëè èíûõ áóêâ â òåêñòå, íà îñíîâàíèè êîòîðîé îáû÷íî î÷åíü ëåãêî âñêðûâàþòñÿ ìîíîàëôàâèòíûå øèôðû.

2. Øèôð Âèæåíåðà

Øèôð Âèæåíåðà (ôð. Chiffre de Vigenère) - ìåòîä ïîëèàëôàâèòíîãî øèôðîâàíèÿ áóêâåííîãî òåêñòà ñ èñïîëüçîâàíèåì êëþ÷åâîãî ñëîâà.

Ýòîò ìåòîä ÿâëÿåòñÿ ïðîñòîé ôîðìîé ìíîãîàëôàâèòíîé çàìåíû. Øèôð Âèæåíåðà èçîáðåòàëñÿ ìíîãîêðàòíî. Âïåðâûå ýòîò ìåòîä îïèñàë Äæîâàí Áàòòèñòà Áåëëàçî (èòàë. Giovan Battista Bellaso) â êíèãå La cifra del. Sig. Giovan Battista Bellaso â 1553 ãîäó, îäíàêî, â XIX âåêå ïîëó÷èë èìÿ Áëåçà Âèæåíåðà, ôðàíöóçñêîãî äèïëîìàòà. Ìåòîä ïðîñò äëÿ ïîíèìàíèÿ è ðåàëèçàöèè, îí ÿâëÿåòñÿ íåäîñòóïíûì äëÿ ïðîñòûõ ìåòîäîâ êðèïòîàíàëèçà.

.1 Èñòîðèÿ

Ïåðâîå òî÷íîå äîêóìåíòèðîâàííîå îïèñàíèå ìíîãîàëôàâèòíîãî øèôðà áûëî ñôîðìóëèðîâàíî Ëåîíîì Áàòòèñòà Àëüáåðòè <#"justify">.2 Îïèñàíèå

Â øèôðå Öåçàðÿ <#"justify">ATTACKATDAWN

×åëîâåê, ïîñûëàþùèé ñîîáùåíèå, çàïèñûâàåò êëþ÷åâîå ñëîâî («LEMON») öèêëè÷åñêè äî òåõ ïîð, ïîêà åãî äëèíà íå áóäåò ñîîòâåòñòâîâàòü äëèíå èñõîäíîãî òåêñòà:

Ïåðâûé ñèìâîë èñõîäíîãî òåêñòà A çàøèôðîâàí ïîñëåäîâàòåëüíîñòüþ L, êîòîðàÿ ÿâëÿåòñÿ ïåðâûì ñèìâîëîì êëþ÷à. Ïåðâûé ñèìâîë L øèôðîâàííîãî òåêñòà íàõîäèòñÿ íà ïåðåñå÷åíèè ñòðîêè L è ñòîëáöà A â òàáëèöå Âèæåíåðà. Òî÷íî òàê æå äëÿ âòîðîãî ñèìâîëà èñõîäíîãî òåêñòà èñïîëüçóåòñÿ âòîðîé ñèìâîë êëþ÷à; òî åñòü âòîðîé ñèìâîë øèôðîâàííîãî òåêñòà X ïîëó÷àåòñÿ íà ïåðåñå÷åíèè ñòðîêè E è ñòîëáöà T. Îñòàëüíàÿ ÷àñòü èñõîäíîãî òåêñòà

øèôðóåòñÿ ïîäîáíûì ñïîñîáîì.

Èñõîäíûé òåêñò:ATTACKATDAWN

Êëþ÷:LEMONLEMONLE

Çàøèôðîâàííûé òåêñò: LXFOPVEFRNHR

Ðàñøèôðîâûâàíèå ïðîèçâîäèòñÿ ñëåäóþùèì îáðàçîì: íàõîäèì â òàáëèöå Âèæåíåðà ñòðîêó, ñîîòâåòñòâóþùóþ ïåðâîìó ñèìâîëó êëþ÷åâîãî ñëîâà; â äàííîé ñòðîêå íàõîäèì ïåðâûé ñèìâîë çàøèôðîâàííîãî òåêñòà. Ñòîëáåö, â êîòîðîì íàõîäèòñÿ äàííûé ñèìâîë, ñîîòâåòñòâóåò ïåðâîìó ñèìâîëó èñõîäíîãî òåêñòà. Ñëåäóþùèå ñèìâîëû çàøèôðîâàííîãî òåêñòà ðàñøèôðîâûâàþòñÿ ïîäîáíûì îáðàçîì.

Åñëè áóêâû A-Z ñîîòâåòñòâóþò ÷èñëàì 0-25, òî øèôðîâàíèå Âèæåíåðà ìîæíî çàïèñàòü â âèäå ôîðìóëû:

Ðàñøèôðîâêà:

Äîïóñòèì, ÷òî íàì íàäî çàøèôðîâàòü íåêèé òåêñò, ïåðâûì ñëîâîì êîòîðîãî ÿâëÿåòñÿ ñëîâî DANCE. Çàøèôðóåì ïåðâûå äâå áóêâû, à âñå îñòàëüíûå äåëàþòñÿ àíàëîãè÷íî. Â ãðàôå «êëþ÷» ìíîãîêðàòíî ïîâòîðÿåì ñëîâî ABC, â ãðàôå «îòêðûòûé òåêñò» ïðèâîäèì îòêðûòûé òåêñò, â ãðàôå «øèôðîâàííûé òåêñò» ïðèâîäèì çàøèôðîâàííûé òåêñò:

Áåð¸ì ïåðâóþ áóêâó è ñìîòðèì, êàêàÿ áóêâà êëþ÷à íàõîäèòñÿ íàä íåé, à çàòåì ïîëó÷åííóþ áóêâó êëþ÷à íàõîäèì â ïåðâîì ñòîëáöå êâàäðàòà Âèæåíåðà, à øèôðóåìóþ áóêâó â ïåðâîé ñòðîêå, çàòåì ñìîòðèì, êàêàÿ áóêâà íàõîäèòñÿ íà ïåðåñå÷åíèè ïîëó÷åííîé ñòðîêè è ñòîëáöà - îíà è áóäåò çàøèôðîâàííîé áóêâîé:

Â ðåçóëüòàòå ïîäîáíûõ îïåðàöèé ïîëó÷àåì DBPCF. Îáðàòèì âíèìàíèå íà òîò ôàêò, ÷òî äëèíà êëþ÷à ðàâíà ÷èñëó âñåõ ìîíîàëôàâèòíûõ øèôðîâ, ñóïåðïîçèöèåé êîòîðûõ ÿâëÿåòñÿ íàø ïîëèàëôàâèòíûé øèôð. Îäíîé èç ìîäèôèêàöèé äàííîãî ìåòîäà ÿâëÿåòñÿ èñïîëüçîâàíèå â êà÷åñòâå êëþ÷à âñåãî îòêðûòîãî òåêñòà (òî åñòü â ãðàôå «êëþ÷» ïðîñòî ïèøåòñÿ ïîäðÿä âåñü èñõîäíûé òåêñò), òîëüêî ñ îäíîé ïîïðàâêîé, íåîáõîäèìîé äëÿ çàïóòûâàíèÿ êðèïòîàíàëèòèêà: ïåðâóþ áóêâó êëþ÷à âûáåðåì ïðîèçâîëüíî, à äàëüøå óæå òåêñò ñîîáùåíèÿ:

.3 Êðèïòîàíàëèç

Øèôð Âèæåíåðà «ðàçìûâàåò» õàðàêòåðèñòèêè ÷àñòîò ïîÿâëåíèÿ ñèìâîëîâ â òåêñòå, íî íåêîòîðûå îñîáåííîñòè ïîÿâëåíèÿ ñèìâîëîâ â òåêñòå îñòàþòñÿ. Ãëàâíûé íåäîñòàòîê øèôðà Âèæåíåðà ñîñòîèò â òîì, ÷òî åãî êëþ÷ ïîâòîðÿåòñÿ. Ïîýòîìó ïðîñòîé êðèïòîàíàëèç øèôðà ìîæåò áûòü ïîñòðîåí â äâà ýòàïà:

1.Ïîèñê äëèíû êëþ÷à. Ìîæíî àíàëèçèðîâàòü ðàñïðåäåëåíèå ÷àñòîò â çàøèôðîâàííîì òåêñòå ñ ðàçëè÷íûì ïðîðåæèâàíèåì. Òî åñòü áðàòü òåêñò, âêëþ÷àþùèé êàæäóþ 2-þ áóêâó çàøèôðîâàííîãî òåêñòà, ïîòîì êàæäóþ 3-þ è ò. ä. Êàê òîëüêî ðàñïðåäåëåíèå ÷àñòîò áóêâ áóäåò ñèëüíî îòëè÷àòüñÿ îò ðàâíîìåðíîãî (íàïðèìåð, ïî ýíòðîïèè), òî ìîæíî ãîâîðèòü î íàéäåííîé äëèíå êëþ÷à.

2.Êðèïòîàíàëèç. Ñîâîêóïíîñòü l-øèôðîâ Öåçàðÿ (ãäå l - íàéäåííàÿ äëèíà êëþ÷à), êîòîðûå ïî îòäåëüíîñòè ëåãêî âçëàìûâàþòñÿ.

Òåñòû Ôðèäìàíà è Êàñèñêè ìîãóò ïîìî÷ü îïðåäåëèòü äëèíó êëþ÷à.

.3.1Ìåòîä Êàñèñêè

Â 1863 ãîäó Ôðèäðèõ Êàñèñêè áûë ïåðâûì, êòî îïóáëèêîâàë óñïåøíûé àëãîðèòì àòàêè íà øèôð Âèæåíåðà, õîòÿ ×àðëüç Áåááèäæ <#"justify">Êëþ÷:ABCDEF AB CDEFA BCD EFABCDEFABCD

Èñõîäíûéòåêñò:CRYPTO IS SHORT FOR CRYPTOGRAPHY

Øèôðîâàííûéòåêñò: CSASXT IT UKSWT GQU GWYQVRKWAQJB

Çàøèôðîâàííûé òåêñò â äàííîì ñëó÷àå íå áóäåò ïîâòîðÿòü ïîñëåäîâàòåëüíîñòè ñèìâîëîâ, êîòîðûå ñîîòâåòñòâóþò ïîâòîðíûì ïîñëåäîâàòåëüíîñòÿì èñõîäíîãî òåêñòà. Â äàííîì øèôðîâàííîì òåêñòå åñòü íåñêîëüêî ïîâòîðÿþùèõñÿ ñåãìåíòîâ, êîòîðûå ïîçâîëÿþò êðèïòîàíàëèòèêó íàéòè äëèíó êëþ÷à:

Êëþ÷:ABCDAB CD ABCDA BCD ABCDABCDABCDÈñõîäíûé òåêñò:CRYPTO IS SHORT FOR CRYPTOGRAPHYØèôðîâàííûé òåêñò:CSASTP KV SIQUT GQU CSASTPIUAQJB

Áîëåå äëèííûå ñîîáùåíèÿ äåëàþò òåñò áîëåå òî÷íûì, òàê êàê îíè âêëþ÷àþò â ñåáÿ áîëüøå ïîâòîðÿþùèõñÿ ñåãìåíòîâ çàøèôðîâàííîãî òåêñòà. Â äàííîì øèôðîâàííîì òåêñòå åñòü íåñêîëüêî ïîâòîðÿþùèõñÿ ñåãìåíòîâ, êîòîðûå ïîçâîëÿþò êðèïòîàíàëèòèêó íàéòè äëèíó êëþ÷à:

Øèôðîâàííûé òåêñò:

Ðàññòîÿíèå ìåæäó ïîâòîðÿþùèìèñÿ DYDUXRMH ðàâíî 18, ýòî ïîçâîëÿåò ñäåëàòü âûâîä, ÷òî äëèíà êëþ÷à ðàâíà îäíîìó èç çíà÷åíèé: 18, 9, 6, 3 èëè 2. Ðàññòîÿíèå ìåæäó ïîâòîðÿþùèìèñÿ NQD ðàâíî 20. Èç ýòîãî ñëåäóåò, ÷òî äëèíà êëþ÷à ðàâíà 20 èëè 10, èëè 5, èëè 4 èëè 2. Ñðàâíèâàÿ âîçìîæíûå äëèíû êëþ÷åé, ìîæíî ñäåëàòü âûâîä, ÷òî äëèíà êëþ÷à (ïî÷òè íàâåðíÿêà) ðàâíà 2.

.3.2 Òåñò Ôðèäìàíà

Òåñò Ôðèäìàíà (èíîãäà íàçûâàåìûé êàïïà-òåñò) áûë èçîáðåòåí Âèëüÿìîì Ôðèäìàíîì â 1920 ãîäó. Ôðèäìàí èñïîëüçîâàë èíäåêñ ñîâïàäåíè <#"justify">

Èç íàáëþäåíèÿ çà ÷àñòîòîé ñîâïàäåíèÿ ñëåäóåò:

ãäå - ðàçìåð àëôàâèòà (26 ñèìâîëîâ äëÿ àíãëèéñêîãî ÿçûêà), - äëèíà òåêñòà, è äî - íàáëþäàåìûå ÷àñòîòû ïîâòîðåíèÿ ñèìâîëîâ çàøèôðîâàííîãî òåêñòà. Îäíàêî, ýòî òîëüêî ïðèáëèçèòåëüíîå çíà÷åíèå, òî÷íîñòü êîòîðîãî óâåëè÷èâàåòñÿ ïðè áîëüøåì ðàçìåðå òåêñòà. Íà ïðàêòèêå ýòî áûëî áû íåîáõîäèìî äëÿ ïåðåáîðà ðàçëè÷íûõ êëþ÷åé ïðèáëèæàÿñü ê èñõîäíîìó.

.4 ×àñòîòíûé àíàëèç

Êàê òîëüêî äëèíà êëþ÷à ñòàíîâèòñÿ èçâåñòíîé, çàøèôðîâàííûé òåêñò ìîæíî çàïèñàòü âî ìíîæåñòâî ñòîëáöîâ, êàæäûé èç êîòîðûõ ñîîòâåòñòâóåò îäíîìó ñèìâîëó êëþ÷à. Êàæäûé ñòîëáåö ñîñòîèò èç èñõîäíîãî òåêñòà, êîòîðûé çàøèôðîâàí øèôðîì Öåçàðÿ; êëþ÷ ê øèôðó Öåçàðÿ ÿâëÿåòñÿ âñåãî-íàâñåãî îäíèì ñèìâîëîì êëþ÷à äëÿ øèôðà Âèæåíåðà, êîòîðûé èñïîëüçóåòñÿ â ýòîì ñòîëáöå. Èñïîëüçóÿ ìåòîäû, ïîäîáíûå ìåòîäàì âçëîìà øèôðà Öåçàðÿ, ìîæíî ðàñøèôðîâàòü çàøèôðîâàííûé òåêñò. Óñîâåðøåíñòâîâàíèå òåñòà Êàñèñêè, èçâåñòíîå êàê ìåòîä Êèðõãîôà, çàêëþ÷àåòñÿ â ñðàâíåíèè ÷àñòîòû ïîÿâëåíèÿ ñèìâîëîâ â ñòîëáöàõ ñ ÷àñòîòîé ïîÿâëåíèÿ ñèìâîëîâ â èñõîäíîì òåêñòå äëÿ íàõîæäåíèÿ êëþ÷åâîãî ñèìâîëà äëÿ ýòîãî ñòîëáöà. Êîãäà âñå ñèìâîëû êëþ÷à èçâåñòíû, êðèïòîàíàëèòèê ìîæåò ëåãêî ðàñøèôðîâàòü øèôðîâàííûé òåêñò, ïîëó÷èâ èñõîäíûé òåêñò. Ìåòîä Êèðõãîôà íå ïðèìåíèì, êîãäà òàáëèöà Âèæåíåðà ñêðåìáëèðîâàíà, âìåñòî èñïîëüçîâàíèÿ îáû÷íîé àëôàâèòíîé ïîñëåäîâàòåëüíîñòè, õîòÿ òåñò Êàñèñêè è òåñòû ñîâïàäåíèÿ âñå åùå ìîãóò èñïîëüçîâàòüñÿ äëÿ îïðåäåëåíèÿ äëèíû êëþ÷à äëÿ ýòîãî ñëó÷àÿ.

.5 Âàðèàíòû

Âàðèàíò running key (àíãë. - áåãóùèé êëþ÷) øèôðà Âèæåíåðà êîãäà-òî áûë íå âçëàìûâàåìûì. Ýòà âåðñèÿ èñïîëüçóåò â êà÷åñòâå êëþ÷à áëîê òåêñòà, ðàâíûé ïî äëèíå èñõîäíîìó òåêñòó. Òàê êàê êëþ÷ ðàâåí ïî äëèíå ñîîáùåíèþ, òî ìåòîäû ïðåäëîæåííûå Ôðèäìàíîì è Êàñèñêè íå ðàáîòàþò (òàê êàê êëþ÷ íå ïîâòîðÿåòñÿ). Â 1920 ãîäó Ôðèäìàí ïåðâûì îáíàðóæèë íåäîñòàòêè ýòîãî âàðèàíòà. Ïðîáëåìà ñ running key øèôðà Âèæåíåðà ñîñòîèò â òîì, ÷òî êðèïòîàíàëèòèê èìååò ñòàòèñòè÷åñêóþ èíôîðìàöèþ î êëþ÷å (ó÷èòûâàÿ, ÷òî áëîê òåêñòà íàïèñàí íà èçâåñòíîì ÿçûêå) è ýòà èíôîðìàöèÿ áóäåò îòðàæàòüñÿ â øèôðîâàííîì òåêñòå. Åñëè êëþ÷ äåéñòâèòåëüíî ñëó÷àéíûé, åãî äëèíà ðàâíà äëèíå ñîîáùåíèÿ, è îí èñïîëüçîâàëñÿ åäèíîæäû, òî øèôð Âèæåíåðà òåîðåòè÷åñêè áóäåò íå âçëàìûâàåìûì.

Âèæåíåð ôàêòè÷åñêè èçîáðåë áîëåå ñòîéêèé øèôð - øèôð <#"justify">.6 Ýêñïåðèìåíòàëüíàÿ ïðîâåðêà ðàáîòû ïðîãðàììû

Äëÿ ïðîâåðêè ðàáîòû ïðîãðàììû, âûïîëíÿþùåé øèôðîâàíèå ïî òàáëèöå Âèæåíåðà, âîçüìåì, íàïðèìåð, ñëîâî «ïðèâåòñòâèå», à êëþ÷åâûì ñèìâîëîì áóäåò ÿâëÿòüñÿ, íàïðèìåð, ñëîâî «äâà».

Ïîñëå øèôðîâàíèÿ áûë ïîëó÷åí ñëåäóþùèé çàøèôðîâàííûé òåêñò:

«ÑÐÌÄÅÖÓÒÆÊÅ»

Äëÿ ïðîâåðêè ðàáîòû ïðîãðàììû äåøèôðîâàíèÿ ïî òàáëèöå Âèæåíåðà âîçüìåì ýòîò æå çàøèôðîâàííûé òåêñò «ÑÐÌÄÅÖÓÒÆÊÅ». Ïðè ýòîì êëþ÷åâûì ñèìâîëîì äîëæíî ÿâëÿòüñÿ ñëîâî «äâà». Ïðè ðàñøèôðîâêå òåêñòà ïîëó÷èì ïåðâîíà÷àëüíûé òåêñò «ïðèâåòñòâèå».

3. Âçëîì ïîëèàëôàâèòíûõ øèôðîâ

Ïðîùå âñåãî âçëîìàòü ïîëèàëôàâèòíûé øèôð, çíàÿ åãî ïåðèîä, òî åñòü ÷èñëî èñïîëüçóåìûõ ìîíîàëôàâèòíûõ øèôðîâ. Òîãäà, âûáðàâ áóêâû, ñîîòâåòñòâóþùèå êàæäîìó èç ìîíîàëôàâèòíûõ øèôðîâ, ìîæíî ê êàæäîìó èç íèõ ïðèìåíèòü òàê íàçûâàåìûé ÷àñòîòíûé àíàëèç (èëè êàêîé-íèáóäü äðóãîé ìåòîä âçëîìà ìîíîàëôàâèòíûõ øèôðîâ). Ìåòîä îñíîâàí íà òîì, ÷òî êàæäàÿ áóêâà â ïðîèçâîëüíîì òåêñòå ïîÿâëÿåòñÿ ñ âïîëíå îïðåäåëåííîé ÷àñòîòîé, à çíà÷èò, ïîñìîòðåâ ÷àñòîòû ïîÿâëåíèÿ òåõ èëè èíûõ áóêâ, ìîæíî óçíàòü, êàê ïðîèñõîäèò çàìåíà. Îäíèì èç ìåòîäîâ íàõîæäåíèÿ ïåðèîäà ïîëèàëôàâèòíûõ øèôðîâ ÿâëÿåòñÿ ìåòîä, ïðåäëîæåííûé Ôðåäåðèêîì Êàñèñêè â 1836 ãîäó. Îí çàêëþ÷àåòñÿ â òîì, ÷òî â çàøèôðîâàííîì òåêñòå íàõîäÿòñÿ îäèíàêîâûå ñåãìåíòû äëèíû íå ìåíüøå, ÷åì òðè áóêâû, çàòåì âû÷èñëÿþòñÿ ðàññòîÿíèÿ ìåæäó ïåðâûìè áóêâàìè ñîñåäíèõ ñåãìåíòîâ. Îêàçûâàåòñÿ, ïðåäïîëàãàåìûé ïåðèîä ÿâëÿåòñÿ êðàòíûì íàèáîëüøåìó îáùåìó äåëèòåëþ äëÿ ýòèõ ðàññòîÿíèé.

Çàêëþ÷åíèå

Â ðåçóëüòàòå âûïîëíåíèÿ êóðñîâîé ðàáîòû áûëà ðàçðàáîòàíà ïðîãðàììà, ðåàëèçóþùàÿ êðèïòîãðàôè÷åñêèé àëãîðèòì øèôðîâàíèÿ è äåøèôðîâàíèÿ ñ èñïîëüçîâàíèåì øèôðà Âèæåíåðà. Ðàçðàáîòàííàÿ ïðîãðàììà íàïèñàíà íà ÿçûêå Delphi ("Äåëôè").

Òàêæå áûëà âûïîëíåíà ýêñïåðèìåíòàëüíàÿ ïðîâåðêà ðàáîòû äàííîé ïðîãðàììû, ïîäòâåðæäàþùàÿ ïðàâèëüíîñòü øèôðîâàíèÿ.

Ñ ðàçâèòèåì ÝÂÌ ïîëèàëôàâèòíûå øèôðû ïåðåñòàëè áûòü ñòîëü óñòîé÷èâûìè ê êðèïòîàòàêàì, è, òàê æå, êàê â ñâîå âðåìÿ è ìîíîàëôàâèòíûå øèôðû, îòîøëè íà çàäíèé ïëàí, ñòàâ ÷àñòüþ èñòîðèè.

Ñïèñîê ëèòåðàòóðû

1.À.Â. ßêîâëåâ, À.À. Áåçáîãîâ, Â.Â. Ðîäèí, Â.Í. Øàìêèí. Êðèïòîãðàôè÷åñêàÿ çàùèòà èíôîðìàöèè. - Òàìáîâ: Èçäàòåëüñòâî ÒÃÒÓ, 2006

2.David, Kahn. On the Origin of a Species. The Codebreakers: The Story of Secret Writing. Simon & Schuster, 1999

3.Henk C.A. van Tilborg, ed. Encyclopedia of Cryptography and Security (First ed.). Springer. pp. 115, 2005

4.Ý. Ì. Ãàáèäóëèí. Êóðñ ëåêöèé ïî Çàùèòå Èíôîðìàöèè. - Ìîñêâà: Èçäàòåëüñòâî ÌÔÒÈ, 2007

.À. Ï. Àëôåðîâ, À. Þ. Çóáîâ, À. Ñ. Êóçüìèí, À. Â. ×åðåìóøêèí. Îñíîâû êðèïòîãðàôèè. - Ìîñêâà: Èçäàòåëüñòâî Ãåëèîñ ÀÐÂ, 2005

Ïðèëîæåíèå À

Øèôð Âèæåíåðà

unit TablVin;

interface, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms, , Grids, ComCtrls, ExtCtrls, StdCtrls, Buttons, Menus, hlp;= class(TForm): TPageControl;: TTabSheet;: TTabSheet;: TStringGrid;: TPanel;: TSpeedButton;: TSpeedButton;: TStringGrid;: TPopupMenu;: TMenuItem;: TEdit;: TLabel;: TMemo;: TMemo;: TSpeedButton;: TSpeedButton;: TSpeedButton;: TSpeedButton;: TStatusBar;: TOpenDialog;: TSaveDialog;: TSpeedButton;: TMainMenu;: TMenuItem;: TMenuItem;: TTimer;: TSpeedButton;: TSpeedButton;: TLabel;: TLabel;: TLabel;: TButton;: TButton;: TMenuItem;: TLabel;: TButton;: TButton;FormCreate(Sender: TObject);N1Click(Sender: TObject);FormClose(Sender: TObject; var Action: TCloseAction);Edit1KeyPress(Sender: TObject; var Key: Char);REd1KeyPress(Sender: TObject; var Key: Char);SG2KeyPress(Sender: TObject; var Key: Char);SB1Click(Sender: TObject);SB2Click(Sender: TObject);REd2KeyPress(Sender: TObject; var Key: Char);SB7Click(Sender: TObject);SB3Click(Sender: TObject);SB5Click(Sender: TObject);N3Click(Sender: TObject);SB4Click(Sender: TObject);SB6Click(Sender: TObject);LokBut(Sender: TObject);SpeedButton1Click(Sender: TObject);SpeedButton2Click(Sender: TObject);Button1Click(Sender: TObject);Button2Click(Sender: TObject);N4Click(Sender: TObject);Button3Click(Sender: TObject);Button4Click(Sender: TObject);

{ Private declarations }

{ Public declarations };= ['a'..'z', '0'..'9'];Rez :TStrings; Old1, Old2 :String;:Set of Char; // Äîïóñòèìûåñèìâîëû: TForm1;Det0(Tb :TStringGrid):Boolean;Invert(S :String; N :LongInt):String;KeyR(Tb :TStringGrid; Zn :Char; N :Integer=0):Integer;KeyS(Tb :TStringGrid; Zn :Char; N :Integer=0):Integer;Znak(Tb :TStringGrid; C, R :LongInt):Char;

{$R \*.dfm}TForm1.FormCreate(Sender: TObject);ColL :LongInt; Lst :TStrings;:= [];:= 0; // Íîëüñòðîê:=TStringList.Create;.Clear;FileExists( ExtractFilePath(ParamStr(0))+'Grid.cfg' ) Then.LoadFromFile( ExtractFilePath(ParamStr(0))+'Grid.cfg' );:= Lst.Count;.RowCount := ColL;.Free;;

//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++.Visible:=False;.ActivePage:=TabSheet2;FileExists(ExtractFilePath(ParamStr(0))+'Grid.cfg') Then.Cols[0].LoadFromFile(ExtractFilePath(ParamStr(0))+'Grid.cfg');

//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++.ColCount := ColL;.RowCount := Sg1.ColCount;

//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++.Click;(REd1.Lines.Count>0)OR(REd2.Lines.Count>0)Then SB7.Enabled:=True ELSE.Enabled:=False;;Det0(Tb :TStringGrid):Boolean;

VAR R :LongInt; //Çàïîëíåíîñòüòàáëèöû

Det0:=True;R:=0 To Tb.RowCount-1 DoTb.Cells[0, R]='' Then:=True;('ÇÀÏÎËÍÈÒÅÂÑ¨!'); Break;ELSE Det0:=False;;TForm1.N1Click(Sender: TObject);R, I :LongInt; Ms, Sd :String;Det0(SG2) Then Exit;

//=============================================== Ôèëüòðñèìâîëîâ:= [];I:=0 To Sg2.RowCount - 1 Do:= Cont + [ Znak(Sg2, 0, I) ];;

//===============================================.Enabled:=False;:='';I:=0 To Sg2.RowCount-1 Do:=MS+SG2.Cells[0, I];R:=0 To SG1.RowCount-1 Do.Rows[R].Clear;:=Invert(MS, R);I:=1 to Length(Sd) Do.Rows[R].Add( Sd[I] );;.Enabled:=True;;TForm1.FormClose(Sender: TObject; var Action: TCloseAction);Det0( Sg2 ) = False Then.Cols[0].SaveToFile(ExtractFilePath(ParamStr(0))+'Grid.cfg');;Invert(S :String; N :LongInt):String;S1, S2, Sum :String;(S='')OR(N>Length(S))Then Exit;

///////////////////////////N>0 Then:=''; S2:='';:=Copy(S, 1, N);:=Copy(S, N+1, Length(S)-N);:=S2+S1;:=Sum;ELSEN<=0 Then:=S;;('ÂÍÓÒÐÅÍßßÎØÈÁÊÀ!'); Exit;;;TForm1.Button1Click(Sender: TObject);.showmodal;;TForm1.Button2Click(Sender: TObject);.Visible:=Not SG1.Visible;;TForm1.Button3Click(Sender: TObject);.ActivePage:=TabSheet1;;TForm1.Button4Click(Sender: TObject);.ActivePage:=TabSheet2;;TForm1.Edit1KeyPress(Sender: TObject; var Key: Char);Key OF

'À'..'ß', #8, #9: ;

'à'..'ÿ', 'a'..'z': Key:=Chr(Ord(Key)-32);

'¸', '¨': Key:='¨';

// ELSE Key:=#0;;Not (Key in Cont) Then Key:=#0;;TForm1.REd1KeyPress(Sender: TObject; var Key: Char);Key OF

'À'..'ß', #8, #9, #13, #10, ' ': ;

'à'..'ÿ', 'a'..'z': Key:=Chr(Ord(Key)-32);

'¸', '¨': Key:='¨';

'0'..'9': ;;;TForm1.REd2KeyPress(Sender: TObject; var Key: Char);Key OF

'À'..'ß', #8, #9, #13, #10, ' ': ;

'à'..'ÿ', 'a'..'z': Key:=Chr(Ord(Key)-32);

'¸', '¨': Key:='¨';

'0'..'9': ;

// ELSE Key:=#0;;;TForm1.SG2KeyPress(Sender: TObject; var Key: Char);Key OF

'À'..'ß', #8, #9, #13, #10, ' ': ;

'à'..'ÿ', 'a'..'z': Key:=Chr(Ord(Key)-32);

'¸', '¨': Key:='¨';

'0'..'9': ;

// ELSE Key:=#0;;;KeyR(Tb :TStringGrid; Zn :Char; N :Integer=0):Integer;

Var R :LongInt; // ÎÁÙÅÅ: ñêàíåð ñòîëáöîâ// Îïðåäåëåíèå íîìåðà ñòðîêè êëþ÷à " 1-ûé ñòîëáåö "

Result:=0;R:=0 To Tb.RowCount-1 Do.ProcessMessages();Tb.Cells[N, R]=Zn Then Begin Result:=R; Break; End;;;KeyS(Tb :TStringGrid; Zn :Char; N :Integer=0):Integer;

Var C :LongInt; // ÎÁÙÅÅ: ñêàíåð ñòðîê// Îïðåäåëåíèå íîìåðà ñòîëáöà:=0;

For C:=0 To Tb.ColCount-1 Do.ProcessMessages();Tb.Cells[C, N]=Zn Then Begin Result:=C; Break; End;;;Znak(Tb :TStringGrid; C, R :LongInt):Char;//:=Tb.Cells[C, R][1];;TForm1.SB1Click(Sender: TObject);I, J, K :LongInt; Key, Txt, Oyt :String; Ch :Char; A, B :Longint;// ØÈÔÐÓÅÒEdit1.Text='' Then Exit;.Enabled:=False;.Enabled:=False;.Enabled:=False;.Enabled:=False;.Enabled:=False;.Enabled:=False;:=Edit1.Text;:=1;.Lines.Clear; //×èñòêàK:=0 To REd1.Lines.Count-1 DoOyt:='';:=REd1.Lines.Strings[ K ]; //ÃðóçèìñòðîêóI:=1 To Length(Txt{REd1.Lines.Text})Do.ProcessMessages(); //

///////////////////////////////{REd1.Lines.Text[I]}Txt[I] in Cont{['À'..'ß', '¨']} Then:=Key[J];:=KeyR(SG1, Ch, 0) ; // Èùåìíîìåðñèìâîëàêëþ÷àâñòîëáöå:=Txt[I]; //REd1.text[I];

B:=KeyS(SG1, Ch, 0) ; // Èùåì íîìåð ñèìâîëà òåêñòà â ñòðîêå

//REd2.Text:=REd2.Text+Znak(SG1, B, A);:=Oyt+Znak(SG1, B, A);J<=Length(Key)-1 Then J:=J+1 ELSE J:=1; //ÏåðåáîðÊëþ÷àELSE//:=Txt[ I ];

//REd2.Text:=REd2.Text+Ch;:=Oyt+Ch;;

///////////////////////////////;.Lines.Add(Oyt);;.Enabled:=True;.Enabled:=True;.Enabled:=True;.Enabled:=True;.Enabled:=True;.Enabled:=True;;TForm1.SB2Click(Sender: TObject);I, J, K :LongInt; Key, Txt, Oyt :String; Ch :Char; A, B :Longint;// ÐÀÑØÈÔÐÎÂÛÂÀÅÌEdit1.Text='' Then Exit;.Enabled:=False;.Enabled:=False;.Enabled:=False;.Enabled:=False;.Enabled:=False;.Clear; //×èñòèì:=Edit1.Text;:=1;K:=0 To REd2.Lines.Count-1 DoOyt:='';:=REd2.Lines.Strings[K];.ProcessMessages(); //I:=1 To Length( Txt ) DO.ProcessMessages();

//////////////////////////////Txt[I] IN Cont{['À'..'ß', '¨']} Then:=Key[J];:=KeyR(SG1, Ch, 0) ; // Èùåìíîìåðñèìâîëàêëþ÷àâñòîëáöå:=Txt[I]; //REd2.text[I];

B:=KeyS(SG1, Ch, A) ; // Èùåì íîìåð ñèìâîëà òåêñòà â ñòðîêå " Main "

//REd1.Text:=REd1.Text+Znak(SG1, B, 0);:=Oyt+Znak(SG1, B, 0);J<=Length(Key)-1 Then J:=J+1 ELSE J:=1; //ÏåðåáîðÊëþ÷àELSE:=Txt[ I ];

//REd1.Text:=REd1.Text+Ch;:=Oyt+Ch;;

//////////////////////////////;.Lines.Add(Oyt);;.Enabled:=True;.Enabled:=True;.Enabled:=True;.Enabled:=True;.Enabled:=True;.Enabled:=True;;TForm1.SB7Click(Sender: TObject);// Óäàëèòüâñ¸REd1.Lines.Count>0 Then REd1.Clear;REd2.Lines.Count>0 Then REd2.Clear;.Enabled:=False; SB1.Enabled:=False;.Enabled:=False; SB4.Enabled:=False;.Enabled:=False;.Panels[0].Text:='';.Panels[1].Text:='';;TForm1.SB3Click(Sender: TObject);

begin.Title:='Îòêðûòü èñõîäíûé òåêñò ...';

IF OD1.Execute Then.Panels[0].Text:=ExtractFileName( OD1.FileName );:=OD1.FileName;.ProcessMessages(); //.FileName:=Old1;.Lines.LoadFromFile( Old1 );; ShowMessage('Íåòäîñòóïàê: '+Old1);.Panels[0].Text:=''; SD1.FileName:='';;.FileName:='';;;TForm1.SB5Click(Sender: TObject);

begin.Title:='Îòêðûòü øèôðîâàííûé òåêñò ...';

IF OD1.Execute Then.Panels[1].Text:=ExtractFileName( OD1.FileName );:=OD1.FileName;.ProcessMessages(); //.Lines.LoadFromFile( Old2 );; ShowMessage('Íåòäîñòóïàê: '+Old2);.Panels[1].Text:='';;.FileName:='';;;TForm1.N3Click(Sender: TObject);.Visible:=Not SG1.Visible;;TForm1.N4Click(Sender: TObject);

begin('Ëîãâèíîâ Ì.Þ 313ÏÈ Êóðñîâàÿ íà òåìó:"Øèôðîâàíèå Âèæèíåðà" 2012');

end;TForm1.SB4Click(Sender: TObject);

Label 0;.Title:='Ñîõðàíèòü Èñõîäíûé òåêñò êàê ...';

IF SBar1.Panels[0].Text='' Then

: IF SD1.Execute Then:=SD1.FileName;.ProcessMessages();.Lines.SaveToFile( Old1 );.Panels[0].Text:=ExtractFileName( Old1 );;ELSEMessageBox(Handle, PChar( 'Åñëèõîòèòåèñïîëüçîâàòüèìåþùèéñÿïóòü'+

#13+'"'+Old1+'"'+

#13' Íàæìèòå " Äà ".' ), 'Ñîõðàíåíèå', \_YESNO+MB\_ICONINFORMATION)=MrYes Then.Lines.SaveToFile(Old1) ELSE GoTo 0;

//SBar1.Panels[0].Text.FileName:='';;TForm1.SB6Click(Sender: TObject);

Label 1;.Title:='Ñîõðàíèòü Çàøèôðîâàííûé òåêñò êàê ...';

IF SBar1.Panels[1].Text='' Then

: IF SD1.Execute Then:=SD1.FileName;.ProcessMessages();.Lines.SaveToFile( Old2 );.Panels[1].Text:=ExtractFileName( Old2 );;ELSEMessageBox(Handle, PChar( 'Åñëèõîòèòåèñïîëüçîâàòüèìåþùèéñÿïóòü'+

#13+'"'+Old2+'"'+

#13' Íàæìèòå " Äà ".' ), 'Ñîõðàíåíèå', \_YESNO+MB\_ICONINFORMATION)=MrYes Then.Lines.SaveToFile( Old2 ) ELSE GoTo 1;

//SBar1.Panels[0].Text.FileName:='';;TForm1.LokBut(Sender: TObject);// ÏðîâåðêàòåêñòîâûõïîëåéREd1.Lines.Count>0 Then.Enabled:=True;.Enabled:=True;ELSEREd1.Lines.Count<=0 Then.Enabled:=False;.Enabled:=False;;REd2.Lines.Count>0 Then.Enabled:=True;.Enabled:=True;ELSEREd2.Lines.Count<=0 Then.Enabled:=False;.Enabled:=False;;(REd1.Lines.Count>0)OR(REd2.Lines.Count>0)Then SB7.Enabled:=True ELSE.Enabled:=False;.Caption:=Format('Òàáëèöà- [R=%d, C=%d]',

[SG1.RowCount, SG1.ColCount]);

// ÌÅÒÎÄÛÄËß" STRINGGRID "DelCol(SG: TStringGrid);I, J :LongInt;// ÓäàëèòüêîëîíêóSG do:= ColCount - 1;[ J ].Clear;I:=J to ColCount - 2 do[ I ].Assign( Cols[ I+1 ] );:= ColCount - 1;;;DelRow(SG: TStringGrid);I, J :LongInt;// ÓäàëèòüñòðîêóSG do:= RowCount - 1; // Ïîñëåäíÿÿñòðîêà[ J ].Clear;I:=J to RowCount - 2 do[I].Assign( Rows[ I+1 ] );:= RowCount - 1;;;InsRow(SG: TStringGrid);// ÂñòàâêàñòðîêèSG do:= RowCount + 1;;InsCol(StrGrid: TStringGrid);// Âñòàâêàêîëîíîê.ColCount := StrGrid.ColCount + 1;;TForm1.SpeedButton1Click(Sender: TObject);

begin // Äîáàâèòü Ñòðîêó äëÿ ñèìâîëîâSG2.RowCount<256 Then

begin( Sg2 );( Sg1 );( SG1 );ELSE Beep;;TForm1.SpeedButton2Click(Sender: TObject);

begin // Óäàëèòü Ñòðîêó äëÿ ñèìâîëîâSg2.RowCount>33 Then

Begin( Sg2 );( Sg1 );( SG1 );ELSE Beep;

end;.

Ïðèëîæåíèå Á

êðèïòîãðàôè÷åñêèé øèôðîâàíèå âèæåíåð ïîëèàëôàâèòíûé

Ñêðèíøîòû ïðîãðàììû

Ïðèëîæåíèå Â

Êâàäðàò Âèæåíåðà (tabula recta)

ABCDEFGHIJKLM NO PQR STU VW XYZAABCDEFGHIJKLM NO PQR STU VW XYZBBCDEFGHIJKLM N O PQRSTUV W X YZACCDE FGHIJKLM NO PQR STU VW XY ZABDDEFGHIJKLM N O PQRSTUV W X YZABCEEFGHIJKLM NO PQR STUVW XY ZABCDFFGH IJKLM N O PQRSTUVW X YZABCDEGGHI JKLM N O PQRSTU VW XY ZABCDEFHHIJKLM N O PQRSTUV W X YZABCDEFGIIJKLM NO PQR STUVW XYZABCDEFGHJJKLM NO PQRSTUVW XYZABCDEFGHIKKLM N O PQRSTU VW XYZABCDEFGHIJLLM NO PQRSTUV W X YZABCDEFGHIJKMM N O PQRSTU V W X Y ZABCDEFGHIJKLNN O PQRSTU V W X YZABCDEFGHIJKLMOO PQRSTU V W XY ZABCDEFGHIJKLM NPPQR STUV W X YZABCDE FGHIJKLM N OQQRSTU V W X Y ZABCDEFGHIJKLM NO PRRSTU V W X Y ZABCDE FGHIJKLM N O PQSSTUV W XY ZABCDEFGH I JKLM NO PQRTTU VW X YZABCDEFGHI JKLM N O PQRSUU V W X Y ZABCDEFGH I JKLM NO PQRSTVV W XY ZABCDE FGHI JKLM N O PQRSTUWW X YZABCDEFGHIJKLM N O PQRSTU VXX Y ZABCDEFGHIJKLM N O PQRSTUV WYY ZABCDEFGH IJKLM NO PQRSTUVW XZZABCDEFGHI JKLM N O PQRSTUVW X Y