Jelgavas novads
Elejas vidusskola

KRIPTOGRĀFIJA

zinātniski pētnieciskais darbs informātikā

Darbu izstrādāja: 11. klases skolnieks Valters Zaļkalns

Darba vadītājs: skolotājs Jānis Tumovs

2014

Eleja

Saturs

IEVADS

Tūkstošiem gadu cilvēkiem ir bijusi vajadzība sūtīt slepenas vēstules. Parasti šie noslēpumi balstījās uz kodiem, ko zināja tikai sūtītājs un saņēmējs. Kamēr zinātāji tos neizpauda, citiem atšifrēt vēstuli bija grūti. Arī mūsdienās drošai informācijas apmaiņai izmanto šifrēšanu.

Pētījuma mērķis: Izpētīt kriptogrāfijas lomu senatnē un mūsdienās; veikt praktisko šifrēšanu, izmantojot datoru.

Pētījuma uzdevumi:

1. Sameklēt, analizēt un apkopot informāciju par kriptogrāfijas pielietošanu senatnē un mūsdienās;
2. Izveidot šifrēšanas programmas un šifrēšanas režģi.

Pētījuma hipotēze:

Droša informācijas apmaiņu starp subjektiem A un B ir iespējama, ja datu šifrēšanā izmanto datoru.

1. Kriptogrāfijas attīstības vēsture

1.1. Šifrēšanas pirmsākumi

Kriptogrāfija (grieķu: *κρυπτός, kryptos* - slepens, *γράφω, gráphō* - rakstīt), arī kriptoloģija, ir informācijas kodēšanas teorijas nozare, kurā izstrādā metodes, lai aizsargātu informāciju pret nevēlamu nolasīšanu. Mūsdienās ar kriptogrāfiju nodarbojas gan matemātikas, gan IT zinātņu pārstāvji. Kriptogrāfijas sniegtās iespējas izmanto bankomātos, un elektroniskajā tirdzniecībā.

Vajadzība šifrēt radās līdz ar rakstību. Senās Indijas, Ēģiptes un Divupes vēsturiskajos dokumentos atrodamas ziņas par šifrēto rakstu sastādīšanas sistēmām un paņēmieniem. Tā seno indiešu manuskriptos ir izklāstīti 64 veidi teksta pārveidošanai, to starpā zīmju rakstīšanas secības jaukšanas noteikumi. Daudzus no šiem veidiem var uzskatīt par kriptogrāfiskiem, tā kā tie nodrošina sarakstes slepenību. Māka veidot slepenrakstus tolaik tika uzskatīta par obligātu cilvēka izglītības prasmi.

Senajā Grieķijā kriptogrāfija uzplauka. Pulkvedis Enejs Taktika izgudroja *Eneja disku*. Nelielā diskā tika izurbti caurumiņi, no kuriem katrs apzīmēja kādu alfabēta burtu. Cauri šiem caurumiem tika izvērts diegs atbilstoši šifrējamā teksta burtu secībai. Atšifrēt tekstu varēja, velkot diegu ārā. Šī it kā primitīvā metode bija noderīga kara apstākļos, jo ziņojuma pārtveršanas draudu gadījumā viegli varēja diegu saraut, tādā veidā iznīcinot sūtījuma saturu. Pēc līdzīga principa darbojās arī *Eneja lineāls*.

Viena no šifrēšanas metodēm, kura tika izmantot līdz pat XX gs. un, kuru aprakstīja Enejs, ir tā sauktais *grāmatu šifrs*. Viņš piedāvāja virs grāmatas attiecīgajiem burtiem izdurt nelielus caurumiņus. Tad zinātājs no šiem burtiem varēja salikt vēstījumu. Vēl viens grāmatu šifrēšanas veids ir vienošanās par iespieddarbu, lapaspušu, rindiņu un burta secīgo numuru rindiņā, tādējādi šifrējot tekstu ar cipariem. [8.]

1.2. Senās šifrēšanas metodes

Polībijs (200 - 118 p.m.e) bija grieķu vēsturnieks, kas atspoguļoja hellēnisma periodu. Polībijs ir aprakstījis sistēmu, kas tiek saukta par "*Polībija kvadrātu*". 5x5 rūtiņu kvadrātā tika sarakstīts kaut kāds alfabēts un vēstījuma teksts kodēts ar burtu koordinātām (skat. 1. att.).

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

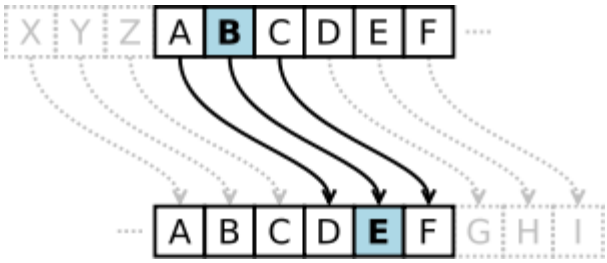
Polībija kvadrāts. 1. attēls.

http://en.wikipedia.org/wiki/Polybius_square

Piemēram, vārds „sveiks” Polībija sistēmā būtu 43 51 15 24 25 43. Protams, burti šifrēšanas kvadrātā jāizvieto haotiski, un slepenraksta saņēmējs jāapgādā ar tādu pašu atšifrēšanas kvadrātu. [9.]

Vēsturiski viens no slavenākajiem kriptogrāfijas pielietojumiem ir romiešu karavadoņa Jūlija Cēzara izveidotais šifrs, ko viņš izmantoja saziņai savā armijā. Cēzara šifrā katrs ziņojuma burts tiek aizvietots ar citu burtu, kas atrodas, piemēram, trīs vietas tālāk alfabētā (skat. 2. att.).

Ja aizkodētais teksts bija garš, tad, zinot valodā lietojamākos burtus, gan Polībija, gan Cēzara šriftu varēja atkodēt salīdzinoši viegli. Tomēr, ja izveido savu alfabētu un maina nobīdes lielumu, atkodēt ziņojumu var tikai, zinot šos divus parametrus.

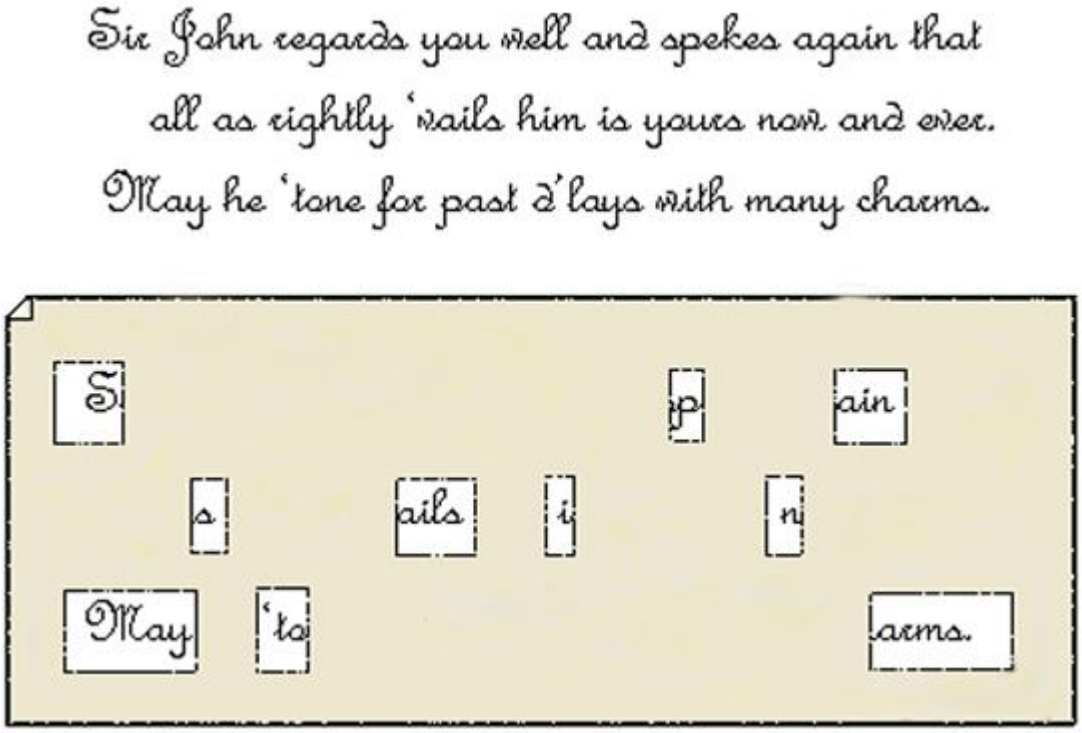


Burtu nobīde Cēzara šifrā. 2. attēls. http://lv.wikipedia.org/wiki/Cēzara_šifrs

Latīņu alfabētā, vārdu LABDIEN kodējot ar soli 3, iegūst ODEGMHQ. Atkodēt var, veicot burtu nobīdi pretējā virzienā par to pašu soli.

Itāļu matemātiķis un filozofs Džerolamo Kardano (1501 – 1576) grāmatā "Par smalkām lietām", aprakstīja šifru, kas mūsdienas pazīstams kā *Kardano režģis*. Tas ir trafarets ar haotiski izvietotiem lodziņiem. Kad trafaretu uzliek uz teksta, pieraksta redzamos burtus. Pēc tam vairākkārt pagriež un pieraksta citus burtus, iegūstot nošifrētu sākotnējo tekstu. [5.]

Džerolamo Kardano. 3. attēls. http://en.wikipedia.org/wiki/Gerolamo_Cardano



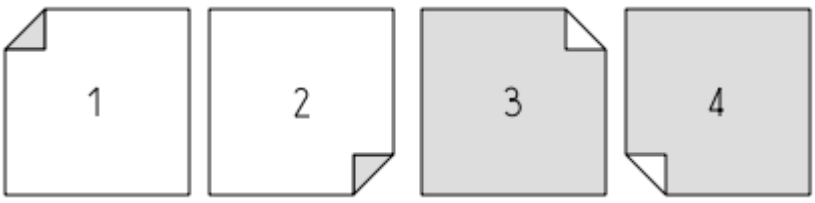
Kardano režģis. 4. attēls. http://en.wikipedia.org/wiki/Cardan_grille

Kardano režģis bija izgatavots no diezgan cieta papīra vai pergamenta loksnes, vai no plāna metāla. Papīrs ir domāts, lai attēlotu rokraksta līnijas un taisnstūra laukumus izgrieztu starp šīm līnijām (skat. 4.att.).

Režģa taisnstūros uz papīra loksnes raksta šifrēto ziņojumu. Var ierakstīt vienu burtu, zilbi vai pat veselu vārdu. Tad, noņemot režģi, fragmenti tiek papildināti, lai izveidotu šifrēto vēstuli. Kardano ierosināja tekstu veidot trīs reizes, lai pārliecinātos ka nav iespējams ieraudzīt apslēptos vārdus.

Ziņojuma saņēmējam ir jābūt identiskam režģim. Režģu kopijas nogriež no sākotnējās veidnes.

Režģi var novietot četrās pozīcijās - uz augšu un uz leju, stāvus un otrādāk, kas palielina šifrēšanas variantu skaitu (skat. 5.attēls).



Kardano režģim četras pozīcijas. 5. attēls. http://en.wikipedia.org/wiki/Cardan_grille

Praksē varētu būt grūti izveidot nevainojamu tekstu ap slepenajiem burtiem, zilbēm vai vārdiem**.** Samākslota valoda pievērstu uzmanību slēptajiem tekstiem. Kardano režģa mērķis ir izveidot ziņu "bez aizdomām". To atviegloja rakstības standartizācijas trūkums 16. gs.

Pat tad, ja atšifrētājam bija aizdomas, ka vēstule satur arī slēptu tekstu, bez režģa to nevarēja uzzināt. [5.]

Interesantu šifrēšanas paņēmienu izgudroja benediktīniešu ordeņa mūks Tritheims (1462 – 1516). Viņa metodi vēl līdz 1914. gadam uzskatīja par neatšifrējamu.

Piemēram, par atslēgas vārdu izvēlamies IKS, un šifrēsim UZMANIES. Vispirms zem šifrējamā vārda vairākas reizes uzraksta atslēgas vārdu IKS. Tad tabulā atrodam kolonnu, kas apzīmēta ar šifrējamo burtu, un rindu, kas apzīmēta ar to atslēgas vārda burtu, kas atrodas zem šifrējamā burta. Kolonnas un rindas krustojumā esošo burtu ierakstām kriptogrammā. [1.]

U Z M A N I E S
I K S I K S I K
F J H I B D M F

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R
T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T
V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V

Tritenheima šifrēšanas režģis. 1. tabula

1.3. Valodniecības metožu pielietošana atšifrēšanā

Ja zināms, ka šifrs izveidots, katru burtu aizstājot ar vienu un to pašu simbolu, tad atšifrēšanu pareizāk sākt, saskaitot, cik bieži katrs simbols sastopams šifrētajā tekstā. Protams, jāzina, kurā valodā teksts tika uzrakstīts pirms šifrēšanas. Burtu relatīvais biežums dažādām valodām ir atšķirīgs. Lielāko Eiropas tautu valodām tie apskatāmi 2. – 4. tabulā. [1; 54]

Angļu valodai		Franču valodai		Spāņu valodai		Vācu valodai	
E	13%	E	17%	EA	13%	E	17%
T	10%	ASITN	7%	OS	8%	NI	8%
AONRIS	7%	RULO	6%	RNID	6%	STRAD	6%
H	5%	D	4%	LCTU	5%	HUG	4%
DLFCMU	3%	CMP	3%	MP	3%	MCLB	3%
GYPWB	2%	VQGFBHJ	1%	BGYVQ HFZJX	1%	OFK	2%
VKXJQZ	0,5%	ZKW	ļoti maz	KW	ļoti maz	WVZP	1%
						JQYX	ļoti maz

Burtu biežums Rietumeiropas valodās. 2. tabula.

О	10,7%	В	5,2%	У	2,3%	Х	1,2%
Е	8,0%	С	5,1%	Ы	1,9%	Ж	1,0%
Ё	0,6%	Д	3,5%	З	1,8%	Ю	0,7%
А	7,7%	Л	3,4%	Ь	1,7%	Ш	0,7%
И	7,2%	М	3,3%	Б	1,6%	Ц	0,4%
Н	6,7%	П	3,2%	Ч	1,5%	Щ	0,3%
Т	6,4%	К	3,0%	Й	1,4%	Э	0,3%
Р	5,3%	Я	2,4%	Г	1,3%	Ф	0,2%

Burtu biežums krievu valodā. 3. tabula

A	11,1%	K	4,1%	J	2,1%	Ļ	0,2%
I	9,3%	M	4,1%	Z	2,0%	F	0,2%
S	8,3%	O	4,0%	B	1,6%	Ž	0,2%
T	6,9%	P	2,9%	C	1,4%	Ķ	0,1%
E	6,4%	D	2,7%	G	1,3%	H	0,1%
R	5,7%	I	2,3%	Š	1,1%	Č	0,02%
U	5,0%	L	2,3%	Ģ	0,4%		
N	4,9%	V	2,2%	Ū	0,4%		
Ā	4,3%	Ē	2,1%	Ņ	0,3%		

Burtu biežums latviešu valodā. 4. tabula

Piemēram, dati par latviešu valodas burtu atkārtošanās biežumu iegūti, analizējot zinātniski tehniska satura tekstus, kuru kopējais garums ir aptuveni 70 000 rakstzīmju.

Protams, atšifrēšana pēc burtu biežuma nebalstās uz viegli programmējamiem algoritmiem, bet gan uz loģiskiem pieņēmumiem un valodnieciskiem spriedumiem.

2. Šifrēšanas procesa automatizācija

2.1. Šifrēšanas mašīna Enigma

Enigma ir portatīva šifrēšanas mašīna, kura tika izmantota slepenu ziņu šifrēšanā. Enigma visā pasaulē tika izmantota ne tikai militārajās operācijās, bet arī komerciāliem mērķiem. Otrā pasaules kara laikā tā visvairāk bija izplatīta nacistiskajā Vācijā. 1932. gadā poļu matemātiķis Marians Rejevskis kopā ar kolēģiem uzlauza Enigmas kodu. Redzot Otrā pasaules kara sākuma neizbēgamību, poļu ģenerālštābs 1939. gada 25. jūlijā nodeva atšifrēšanas algoritmu angļu un franču izlūkdienestiem. Tāpēc antihitleriskā koalīcija spēja atšifrēt daudzas slepenas ziņas, kuras bija šifrētas (skat. 6. att.)

Enigmas šifrēšanas mašīna bija prasmīgi izveidota, viņa bija, gan ļoti jaudīga, gan ērti lietojama. Tā ir elektromehāniska mašīna, kas atgādina rakstāmmašīnu, ar spraudņplāksni, kas samaina burtus, un rotoriem, kas sajauc alfabētu un lampu panelis, kas parāda rezultātus. Lielākai daļai Enigmas modeļu ir 3 vai 4 rotori ar reflektoru, tas atļauj izmantot tos pašus iestatījumus, ko izmanto šifrēšanā un atšifrēšanā.

Teorētiski atslēgas vārda garums ir $3 \cdot 10^{114}$. Šis skaitlis ir daudz lielāks nekā atomu skaits Visumā. Nacistu lietotais atslēgas vārda garums bija 10^{23}. Tas nozīmē, ka 100000 mehāniķi, katrs pārbaudot vienu atslēgas opciju sekundē, koda uzlaušanu paveiktu divreiz ilgākā laikā nekā pastāv Visums. Neskatoties uz mazajām izredzēm, sabiedrotie centās to izdarīt.

Enigma šifrēšanas mašīna. 6. attēls. http://ciphermachines.com/enigma

Enigma šifrēšanas mašīnu izveidoja vācu inženieris, Artūrs Scherbius, un patentēja 1918. gada 23. februāri. Viņš sākumā mēģināja pārdot savu šifra mašīnu vācu armijai, bet tā neizrādīja interesi. Tāpēc inženieris nolēma izveidot uzņēmumu Enigmas komerciālai ražošanai.

Pirmo reizi pārdošanā Enigmas mašīnas A un B modeļi parādījās 1923. gadā. No tiem nopirka tikai dažus. Tie svēra 50 kg, un bija grūti izmantojami.

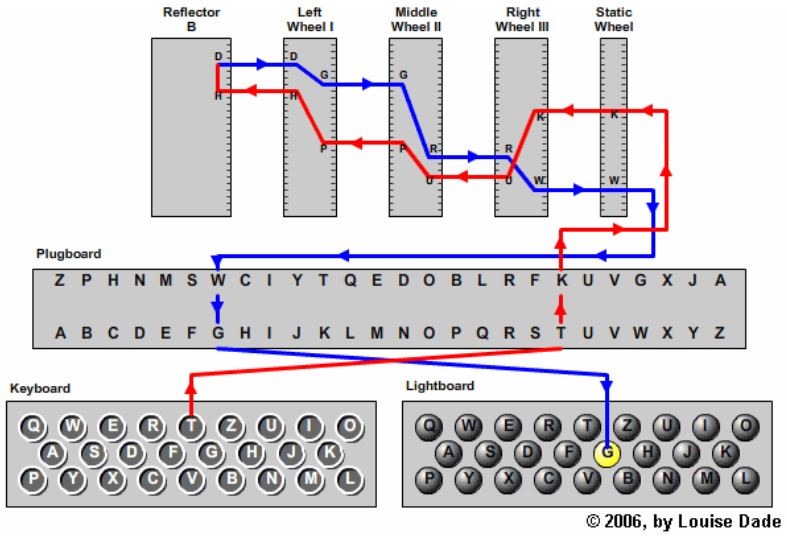
C modelis iznāca 1925. gadā. Tas bija daudz mazāks un vieglāks par iepriekšējiem. D modelis parādījās 1927. gadā. Par to daudzas valstis izrādīja komerciālu interesi.

Vācu kara flote pārņēma Enigmu 1926. gadā, bet armija 1928. gadā. Vācieši Enigmu turpināja izmantot līdz Otrā pasaules kara beigām. Ap šo laiku Enigma svēra tikai 12 kg, daudz mazāk par oriģinālo mašīnu, bet Enigma bija tāpat pārāk smaga karalaukam. Šī šifra mašīna toties bija daudz jaudīgāka par ASV izmantoto M-209. Toties amerikāņu šifra mašīna svēra tikai 2,7 kg. Tai nevajadzēja baterijas, un apkalpei pietika ar vienu cilvēku.

Tastatūrai ir QWERZUI izkārtojums, bez cipariem, atstarpes un simboliem. Spiežot taustiņu, rodas elektrisks signāls, kas mehāniski iekustinās 1 līdz 3 rotorus. Enigmai nav printera, tāpēc tos burtus, kuri iedegās lampu panelī, bija jānoraksta. Katrs burts nošifrēsies no 7 līdz 9 reizēm, un neviens burts nenošifrēsies par sevi.

Elektroinstalācijas diagramma

"T" taustiņu nospiešanas, izraisot 9 šifrēšanas, tad "G" iedegas burts uz lampu paneļa (skat. 7.att.)



Signāla ceļš caur Enigmas mehānismu 7. attēls. http://enigma.louisedade.co.uk/howitworks.html

Šajā gadījumā, spiežot burtu „T", tas ejot cauri spraudņplāksnei pāršifrējas par „K". Ejot cauri rotoriem burts vairakkārt pāršifrējas par kādu citu burtu. Galu galā tas tagad ir burts „H". Tagad signāls atrodas reflektorā un iet atkal uz rotoriem, kur tas šifrējas par citiem burtiem. Tagad signāls ir burts „W", bet, tam ejot cauri spraudņplāksnei, „W" ir savienots ar „G", tāpēc signāls tagad ir „G". Galu galā rezultāts ir redzams uz lampu paneļa, kura oriģināla nozīme ir burts „T", bet kurš pāršifrēts pat „G".

Enigmas mašīnas operatori noraksta burtus, no lampu paneļa un tad tos sūta prom kā šifrētu ziņu. [6.]

Enigma šifru mašīnā lietotājam vajadzēja mainīt iestatījumus katru dienu. Tas nozīme, ka noteiktā secībā tika uzstādīti 3 no 5 rotoriem. Spraudņplāksnē ar kabeļiem savienoti 10 burtu pāri. Visi ikdienas iestatījumi glabājās kodu grāmatā, kuru mainīja reizi mēnesi, bet uz kuģiem un zemūdenēs retāk.

Kaujas laukā vācieši parasti šifrēšanai izmantoja divus cilvēkus – viens raksta uz Enigmas šifru, tikmēr otrs ātri noraksta šifru no lampu paneļa. Reizēm bija trešā persona, kas uzreiz šifrēto tekstu sūtīja radio operatoram (skat. 8. attēlu).

Enigmas izmantošana kara laukā. 8. attēls http://ciphermachines.com/enigma

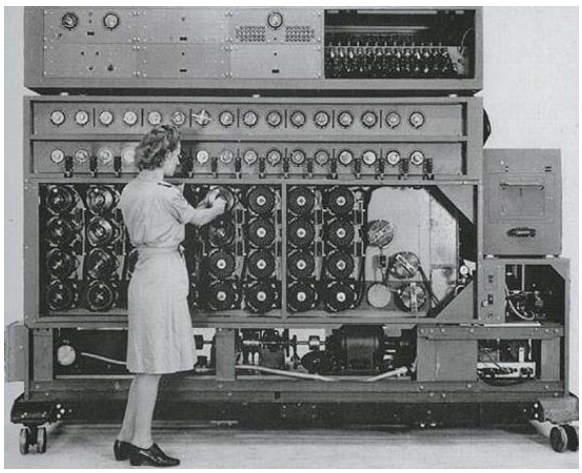
Enigmas šifra komplicētība nacistiem deva pilnīgu pārliecību par ziņojumu drošumu. Pat, redzot pierādījumus, ka Enigmas ziņa uzlauzta, viņi atteicās noticēt, un novēla vainu uz spiegiem vai sagadīšanos. Tas, ka neviens burts nevarēja pāršifrēties pa sevi un katrreizēja 10 kabeļu izmantošana maināmajos burtu pāros, palīdzēja sabiedrotajiem šifru uzlauzt.

1932. gadā Polijas pretizlūkošanas birojs nolīga poļu matemātiķi Marianu Rejevski, lai uzlauztu vācu armijā lietoto šifra mašīnu. Izmantojot arī spiegu palīdzību, šifrēšanas princips tika atklāts.

Poļi izgudroja pirmo elektromehānisko atšifrēšanas mašīnu, lai sistemātiski atkodētu Enigmas ziņojumus. 1938. gada beigās tā sastāvēja no sešām Enigmas mašīnām, lai visi 6 iespējamie rotora uzstādījumi tiktu testēti vienlaikus. Lietojot šo ierīci, Poļi varēja noteikt Enigmas rotora uzstādījumus un atšifrēt nacistu ziņojumus divu stundas laikā. Kad Polijas tika okupēta, nacisti pievienojas vel 2 rotorus, palielinot iespējamo kombināciju skaitu rotora pagriezieniem no 6 līdz 60. Tas padarīja poļu atšifrēšanas mašīnu neefektīvu.

Pēc Vācijas iebrukuma Polijā, visas ziņas un iekārtas Enigmas kodu atšifrēšanai tika nodotas angļu un franču sabiedrotajiem.

Lielbritānijā ar Enigmas atšifrēšanu slepeni nodarbojās vairāk nekā 11000 cilvēku, kurus vadīja matemātiķis Alans Tjurings. Izmantojot poļu pieredzi ar atšifrēšanas mašīnas veidošanu, viņi 1940. gada maijā izveido jaunu atšifrēšanas mašīnu no 36 Enigmām (skat. 8. att.).



Tjuringa atšifrēšanas mašīna. 9. Attēls. http://ciphermachines.com/enigma

Briti regulāri uzlauza Vācijas Gaisa spēku Enigmu mašīnas ziņojumus no 1940. gada līdz kara beigām. Taču ar sauszemes armiju un floti tas neizdevās.

Pirms ASV pievienojās karam, nacistu zemūdenes bija lielākais drauds Lielbritānijai, jo nogremdēja vidēji 60 kuģus mēnesī. Tā kā kuģi no ASV nāca lielos konvojos, tiem vienlaikus uzbruka vairākas vācu zemūdenes. Šī stratēģija bija tik efektīva, ka Vinstons Čērčils teica: „Vienīgā lieta, kas mani patiešām biedēja karā bija vācu zemūdeņu uzbrukums". Nacistu stratēģija bija pilnīgi bloķēt Britu salas, okupēt visu Eiropu pirms ASV iesaistās Otrajā pasaules karā.

1941. gada maijā briti notvēra vācu zemūdeni „U-110", un dabūja kodu grāmatu ar Enigmas uzstādījumiem. Vēlāk briti ieguva arī citas kodu grāmatas, kad uzzināja, ka šifrēšanas mašīnas ir arī uz viegli bruņotajiem vāciešu meteoroloģiskā dienesta kuģiem. Lai vācieši neuzzinātu, ka kodu grāmatas ir pie ienaidnieka, sabiedrotie ievēroja vislielāko slepenību. Tā kā Vācijai nebija aizdomu, Enigmas kodu grāmatas netika nomainītas.

Rezultātā sabiedrotie uzzināja vācu zemūdeņu uzbrukuma mērķus, un ar lidmašīnām tās iznīcināja. Vācijas zaudēja 725 no 1155 zemūdenēm un 82% no 35000 jūrniekiem. [2.][14.]

2.2. Cēzara algoritms datorprogrammās

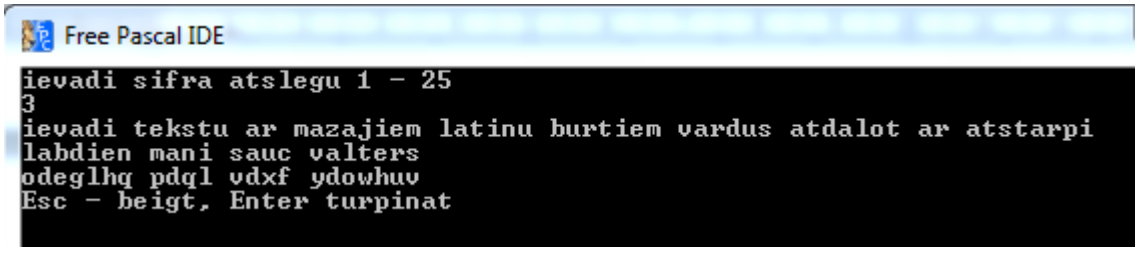
Autors darba praktiskajā daļā ir izveidojis trīs Pascal programmas, kas šifrē un atšifrē ziņojumus pēc Cēzara algoritma.

Pascal ir no visvairāk pazīstamajām programmēšanas valodām. Tā ir bāze un pamats daudzām citām programmēšanas valodām. Pascal izveidoja Niklauss Virts 1968. - 1969. gadā.

Darba autora programmās izmantots latīņu alfabēts, nevis modificētais latīņu alfabēts, kuros ir burti ar diakritiskajām zīmēm, jo Cēzara algoritms vieglāk realizējams ASCII[1] kodos.

Cēzara algoritmi tika programmēti vasarā, jo tas prasīja diezgan daudz laika. Programmēšanas zināšanas autors guva, mācoties LLU Neklātienes programmēšanas skolā 10. klasē, kā arī no darba vadītāja.

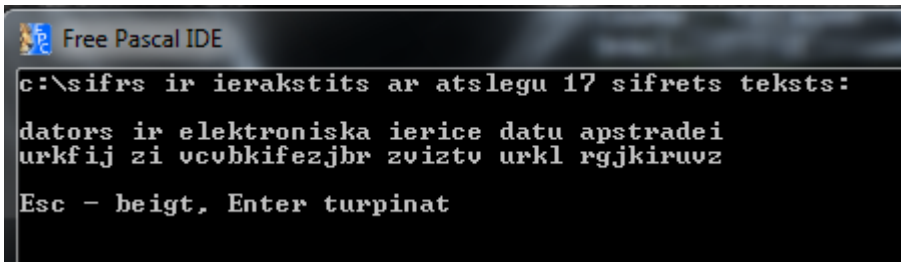
Pirmā programma, ko autors izveidojis, ir SIFRS1. Šī programma lietotājam pieprasa ievadīt skaitli no 1- 25, kas ir šifra atslēga. Ievadot atslēgu, programma pārbīdīs alfabētu par attiecīgu burtu skaitu. Piemēram, ja atslēga ir 3, tad burts „a" būs „d". Pēc šifra atslēgas ievadīšanas programma pieprasīs ievadīt tekstu ar mazajiem burtiem. Pēc ENTER nospiešanas, programma izvadīs rezultātus (skat. 10. att).



Programma SIFRS1. 10. attēls

Kaut arī programmas kods sastāv tikai no 45 rindiņām, autoram šis bija grūts uzdevums.

Otrā autora programma SIFRS2 nejauši izvēlēsies kādu skaitli no 1 līdz 25 un nošifrēs tekstu „dators ir elektroniska ierīce datu apstrādei" ar attiecīgo atslēgu. Pēc teksta izvadīšanas programma piedāvā šifrēšanu atkārtot ar ENTER vai beigt ar ESC. Turpinot darbu, programma atkal nejauši izvēlēsies kādu skaitli no 1 līdz 25 un atkal teksts tiks šifrēts ar attiecīgo atslēgu. Lai mainītu šifrējuma saturu, SIFRS2 kodā, ir jāieraksta cita mainīgā *teksts* vērtība.

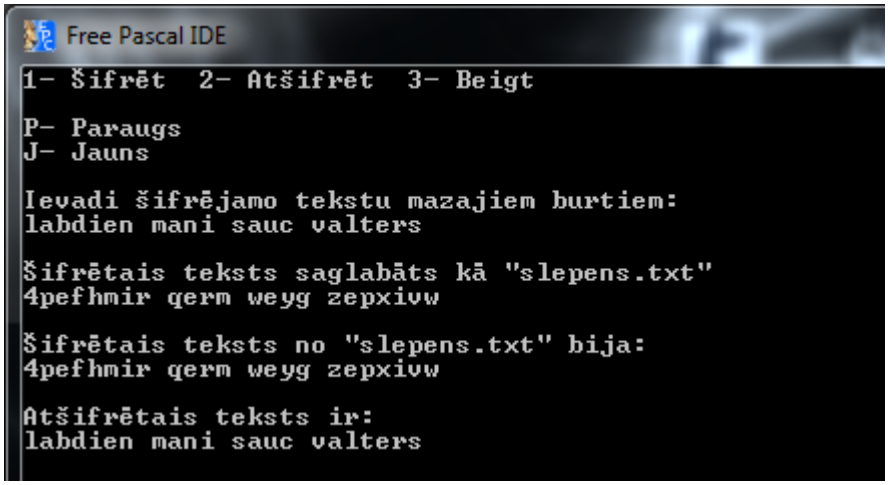


Programma SIFRS2. 11. attēls.

Trešā autora programma ir SIFRS3. Kā iepriekšējās, arī tā balstās uz Cēzara algoritmu. Šī programma autoram sagādāja vislielākās grūtības un aizņēma visvairāk laika. SIFRS3 spēj gan šifrēt, gan atšifrēt, kā arī piedāvā šifrēšanas paraugu. Atverot programmu, tās lietotājam

[1] Amerikas informācijas apmaiņas standartkods latīņu alfabētam

vajadzēs izvēlēties „1” vai „2” vai „3” (skat. 12. att.). Ņemot „3”, programma izslēgsies; ņemot „2”, programma atšifrēs pēdējo šifrējumu. Ņemot „1”, programma piedāvās izveidot jaunu šifru, vai arī parādīs kāda šifra paraugu. Paņemot „Jauns”, programma pieprasīs, lai lietotājs ievada tekstu, kuru vajag nošifrēt. Ievadot tekstu un uzspiežot ENTER, programma nošifrēs tekstu ar nejauši izvēlētu atslēgu. Programma šifrēto tekstu saglabās datnē *slepens.txt*, lai pēc tam, varētu to atšifrēt.



Programma SIFRS3. 12.attēls.

Autora programmas praktiski izmantojamas svarīgas informācijas drošai glabāšanai datorā vai sūtīšanai pa e-pastu. Pirmajā gadījumā pašam jāatceras šifra atslēga jeb skaitlis, kas lielāks par 2 un mazāks par burtu skaitu šifra alfabētā. Otrajā gadījumā ziņojuma adresātam vajadzīga tāda pati datorprogramma un Cēzara šifra atslēga.

Mūsdienās datoru lietotājiem kopumā jāreģistrējas daudzās interneta vietnēs. Parasti tas notiek, norādot atšķirīgus piekļuves datus. Tāpēc daudzās paroles un lietotājvārdus ir grūti atcerēties. Turklāt, paroles ir regulāri jāmaina.

Autora programma varētu atrisināt šo problēmu, jo katru paroli var nošifrēt ar Cēzara algoritmu un droši glabāt datorā teksta datnes formā.

Otrs piemērs ir vēlēšanu rezultātu nosūtīšana no balsošanas iecirkņiem uz centru. Sākotnēji teksta datnes ar rezultātiem, kas bija jāsūta Centrālajai vēlēšanu komisijai, bija visiem lasāmā formā, tātad – nedrošas. Aizpagājušajās pašvaldību vēlēšanās rezultāti jau bija nošifrēti pēc kaut kāda algoritma. Tikpat labi tas varētu būt Cēzara algoritms.

Ko darīt tālāk

Autora datorprogrammas iespējams pilnveidot. Pašreiz tās domātas algoritma būtības demonstrēšanai. Reāli izmantojot, šifra atslēgu nevajag sūtīt kopā ar nošifrēto ziņojumu. Pašreiz tiek izmantots latīņu alfabēts ar burtiem pēc kārtas. Tas hakerim dod iespēju uzminēt šifra veidu un pārbaudīt visas iespējamās atslēgas, lai slepeno tekstu uzlauztu.

Turpmākie datorprogrammu uzlabojumi augstāka līmeņa kriptogrammu iegūšanai varētu būt šādi:

1) šifrēšanas alfabētā latīņu burtu secība ir haotiski sajaukta ar gadījuma skaitļu ģeneratora palīdzību;

2) nav vārdu atstarpju, vai arī tās ir nepareizās vietās;

3) alfabētu un šifrēšanas atslēgu izvada atsevišķi no kriptogrammas;

4) atrast iespēju šifrēšanā izmantot arī latviešu burtus ar diakritiskajām zīmēm.

SIFRS3 koda paraugs apskatāms 2. pielikumā.

3. Elektronisko datu šifrēšana

3.1. Datu drošība informācijas nesējos

Pateicoties informācijas tehnoloģiju straujajai attīstībai, 20. gadsimta beigās būtisku lomu ieguva datu šifrēšana. Tas nozīmē, ka dati tiek nokodēti un bez atkodēšanas nav izlasāmi. Datu šifrēšana ir labāks paņēmiens nekā tikai aizsardzība ar paroli.

Tā kā šifrēšanas programmu algoritmi un šifru atslēgas nav uzlaužamas, „datu šifrēšana daļēji vai pilnībā ir aizliegta tādās valstīs kā Baltkrievijā, Ķīnā un Krievijā" [3.], jo tiesībsargājošie orgāni tad nevar kontrolēt tiem nepieciešamos elektroniskos datus.

Katrai organizācijai vai indivīdam ir dati, kurus jāsargā no neautorizētas piekļuves.

Pirmkārt, būtu jāšifrē portatīvo datoru cietie diski, jo to izmantošana arvien palielinās. Diemžēl aug arī nozagto un pazaudēto datoru skaits. Bieži vien informācija datorā ir vērtīgāka nekā pats dators. Tās zaudēšana vai nonākšana noziedznieku rokās var radīt materiālu un morālu kaitējumu.

Otrkārt, būtu jāšifrē konfidenciālā informācija, kura tiek glabāta uz koplietošanas serveriem. Vairāk nekā 70 procentu no visiem drošības incidentiem notiek, nevis kādam ielaužoties datortīklā no ārpuses, bet gan pateicoties tam, ka organizācijā strādā negodprātīgs darbinieks, kurš palīdz piekļūt konfidenciālai informācijai. Tās šifrēšana ir vienīgais efektīvais veids šī riska būtiskai samazināšanai.

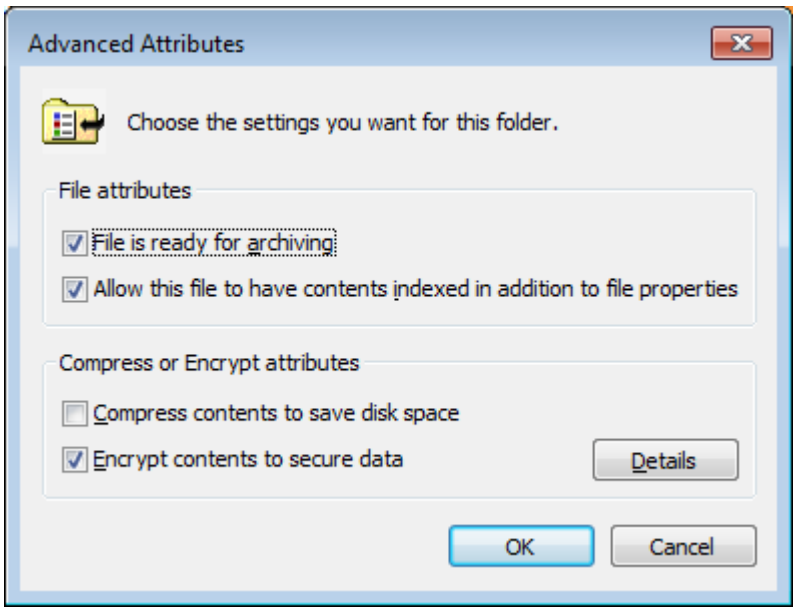
Datu šifrēšanu var veikt ar speciālām programmām, piemēram PGP (Pretty Good Privacy) Desktop palīdzību. [3.]

Jācenšas izmantot tīmekļa vietnes ar drošām datu pārraides tehnoloģijām, piemēram, Secure Sockets Layer (SSL) vai Secure HTTP (SHTTP). Tādējādi, caur Internetu sūtītā informācija tiks šifrēta. [13.]

Operētājsistēmas Windows7 profesionālajās versijās ir ietverta datņu un mapju šifrēšana Encrypting File System (EFS). Tā jāizmanto, lai cietā diska saturs būtu drošībā.

Klikšķiņām labo pogu un izvēlamies datnes vai mapes *Properties*. Ņemam *Advanced* cilnē *General* un atzīmējam *Encrypt contents to secure data*. (skat. 13. att.)

Nošifrēto datņu vai mapju nosaukumi Windows 7 logos attēlosies zaļā krāsā, nevis melnā kā parasti.



13. attēls. Datu šifrēšanas iestatīšana Windows 7

Ar pogu Details var aplūkot, kam būs tiesības šo datni atvērt. Piemēram, domēna lietotāja *Skolotajs* šifrētos dokumentus nevarēs skatīt lietotājs *Skolnieks*.

3.2. RSA šifrēšanas algoritms

RSA šifrēšanas algoritms ir mūsdienās visplašāk lietotais asimetriskās šifrēšanas algoritms. Tā pamatlicēji septiņdesmitajos gados bija ASV kriptogrāfi V. Diffi un M. Helmans. Publiskās atslēgas asimetriskums izpaužas tādējādi, ka kriptogrammas atšifrēšanas algoritms no šifra atslēgas iegūstams vienīgi ar milzīga apjoma skaitļojumu palīdzību. Tātad šifra atslēgas zināšana tikpat kā neko nedod.

Nosaukums RSA ir veidots no tā izgudrotāju uzvārdu pirmajiem burtiem (Rivest, Shamir, Adleman). [11]

RSA algoritmā tiek lietotas divas atslēgas: privātā un publiskā. Datus, kas nošifrēti ar vienu atslēgu, atšifrēt var tikai ar otru. Abas atslēgas ir savā starpā saistītas, bet no vienas aprēķināt otru ir gandrīz neiespējami (šī darbība ir atslēgas atlaušana). Privāto atslēgu tur slepenībā. Publisko atslēgu izplata visiem, kam var būt nepieciešamība nosūtīt šifrētus datus privātās atslēgas turētājam.

Datu šifrēšanai izmanto publisko atslēgu, atšifrēšanai – privāto atslēgu. Elektroniskajam parakstam šifrē ar privāto atslēgu, bet atšifrē ar publisko.

Asimetriskie algoritmi ir ievērojami lēnāki nekā simetriskie, piemēram, AES[2]. Tas ir tāpēc, ka simetriskās šifrēšanas algoritmiem drošas atslēgas garums ir, sākot no 128 bitu skaitļa. Toties RSA vajag jau vismaz 1024 bitus. Atslēgu drošību raksturo laiks, kas

[2] Advanced Encryption Standard

nepiecuiešams tās atrašanai, izmantojot datoru. Ar garākām atslēgām datora darbības notiek lēnāk. Tāpēc lielu informācijas apjomu šifrēšana ar RSA ir apgrūtinoša.

Pietiekoši garu atslēgu (4096 un vairāk) atlaušanai ar klasiskajiem datoriem vajadzētu miljardiem gadu, taču uzskata, ka tādas varētu atlauzt ievērojami īsākā laikā ar kvantu datoru[3]. Pagaidām pietiekoši jaudīgi kvantu datori nav uzbūvēti. Latvijā pie tā veiksmīgi strādā profesors Andris Ambainis.

Līdz 2011. gada jūlijam garākā publiski zināmā atlauztā RSA atslēga ir 768 bitus gara, ko paveica aptuveni 2,5 gados. [12.]

RSA šifra atslēgu veido divu skaitļu pāris (e, n), atšifrēšanas atslēgu – skaitļu pāris (d, n). Slepenībā tiek saglabāta informācija par diviem milzīgiem pirmskaitļiem p un q, kuru reizinājums veido skaitli n. Ja ienaidnieks zina šifrēšanas atslēgu (e, n), bet nezina nevienu no pirmskaitļiem, viņam jāveic milzīgs skaitļošanas darbs, lai izrēķinātu atšifrēšanas atslēgas svarīgo komponentu, t. i., skaitli d. Pati šifrēšanas procedūra paveicama tikai ar atslēgas skaitļu e un n palīdzību, neizmantojot nevienu no slepenībā glabātajiem pirmskaitļiem. [12.]

3.3. E-paraksts

Elektroniskais paraksts ir elektroniski dati, unikāls personas identifikācijas apliecinājums, kas pievienoti datorā sagatavotam dokumentam (vārds, uzvārds, personas kods u.c.). Tādā veidā e-paraksts apliecina tā piederību konkrētai fiziskai personai. Fiziska persona var pārstāvēt juridisku personu

Ar elektroniskais parakstu cilvēks paraksta elektroniskus dokumentus, neizdrukājot tos, piemēram, līgumus, rēķinus, sūdzības, iesniegumus, vēstules u.c., un tam ir juridisks spēks. Parakstot dokumentu, e-paraksta lietotājs piekrīt tā saturam un apliecina savu gribu. E-parakstu var lietot tikai tā īpašnieks.

Ar drošu e-parakstu parakstītam dokumentam ir tāds pats juridiskais spēks kā papīra parakstītam dokumentam.

Kopā ar e-parakstu, komunikācijā ar valsts un pašvaldību iestādēm, atbilstoši likumdošanai ir jālieto laika zīmogs, kas elektroniski fiksē un apliecina konkrētu dokumenta parakstīšanas laiku. Citu dokumentu parakstīšanai laika zīmoga lietošana ir brīvprātīga. Virtuālajā e-parakstā laika zīmogs ir jau iekļauts parakstā.

E-paraksts nav cilvēka fiziskā paraksta grafiskais attēlojums. Tā ir tikai speciāla veida informācija, kas pievienota elektroniskam dokumentam. [7.][4.]

[3] Atšķirīgi gaismas kvantu stāvokļi nozīmē 0 vai 1

SECINĀJUMI

1. Šifrēšana ir izmantota visos laikos.
2. Daudzi šifrēšanas algoritmi balstās uz matemātiskiem principiem un tāpēc ir automatizējami.
3. Šifrēšanas mašīna Enigma bija ievērojams sasniegums pirms datoru izgudrošanas.
4. Programmējot Pascal vidē, iespējams izveidot un atšifrēt slepenus ziņojumus.
5. Šifrēšana pagaidām sniedz drošību informācijas glabāšanā datoros un tās apmaiņā caur Internetu.

IZMANTOTĀ LITERATŪRA

1. E.Riekstiņš, A.Andžāns. Atrisini pats! Zvaigzne 1984, 271 lpp.
2. Cipher Machines [Elektroniskais resurss] - http://ciphermachines.com/enigma
3. Datu šifrēšana – vienīgais drošais veids [Elektroniskais resurss] - http://www.sakaru-pasaule.lv/main.php3?sub=view&RID=1525
4. Elektroniskais paraksts [Elektroniskais resurss] - http://economic.lv/elektroniskais-paraksts/
5. Gerolamo Cardano [Elektroniskais resurss] - http://en.wikipedia.org/wiki/Gerolamo_Cardano
6. How Enigma Machines Work [Elektroniskais resurss] - http://enigma.louisedade.co.uk/howitworks.html
7. Kas ir elektroniskais paraksts [Elektroniskais resurss] - http://www.freewebs.com/guncy-files2/ekomercija-grundstoks-eparaksts.pdf
8. Kriptogrāfija cauri gadsimtiem [Elektroniskais resurss] - http://fizmati.lv/zinas/datorika/kriptografija_cauri_gadsimtiem
9. Polybius [Elektroniskais resurss] - http://en.wikipedia.org/wiki/Polybius
10. Public Keys and Private Keys [Elektroniskais resurss] - http://www.comodo.com/resources/small-business/digital-certificates2.php
11. RSA algoritms [Elektroniskais resurss] - http://lv.wikipedia.org/wiki/RSA_%C5%A1ifr%C4%93%C5%A1anas_algoritms
12. Slepenas informācijas apmaiņas drošība [Elektroniskais resurss] - http://www.sakaru-pasaule.lv/main.php3?sub=view&RID=804
13. Šifrēšanas programmas [Elektroniskais resurss] - http://www.netsafe.lv/page/67
14. The Enigma [Elektroniskais resurss] - http://www.codesandciphers.org.uk/enigma/enigma3.htm

ANOTĀCIJA

Darba autors: Valters Zaļkalns

Darba tēma: Šifrēšanas algoritmi un šifru izmantošana

Darba vadītājs: Jānis Tumovs

Darba apjoms: 26 lappuses

Pētījuma mērķis: Izpētīt kriptogrāfijas lomu senatnē un mūsdienās; veikt praktisko šifrēšanu izmantojot datoru.

Darba saturs: Darbs sastāv no ievada, galvenās daļas (3 nodaļas), secinājumiem, literatūras saraksta, anotācijām un pielikuma. Darbā aprakstīta šifru attīstības vēsture un doti šifru darbības piemēri.

Pētījuma metodes: Darbā izmantota analītiskā un sintēzes pētījuma metode.

Darba rezultāti: 1) Autors izzināja resursos pieejamo informāciju par kriptogrāfiju.
2) Autors iepazinās Enigmas vēsturi un darbības principiem.
3) Autors izveidoja 3 Pascal programmas par šifrēšanu.

Atslēgas vārdi: Šifri, Enigma, Pascal, programmēšana

ANNOTATION

Author: Valters Zaļkalns

Theme: The use of encryption

Scientific tutor: Jānis Tumovs

Size: 26 pages

Aim: Discover role of cryptography in ancient and modern times;
Make a practical encryption using computer.

Content: The work consists of introduction, main part (3 chapters), conclusions, and list of literature, an annotation and a supplement. In the work the history of encryption is described, and also there are given some examples of encryption.

Method of research: In the process methods of analyzing, syntheses and research are used.

Results: 1) The Author finds out available information about cryptography.
2) The Author got acquainted with Enigma history and principles of operation.
3) The Author has created a 3 Pascal programs about encryption.

Keywords: Encryption, cipher, Enigma, Pascal, programming

PIELIKUMS

1. pielikums

Geheime Kommandosache!
Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

№ 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SB	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	YI	nci	oid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	ccc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jhx	uuh	giw	ugw
St	25.	V	IV	III	13	04	17	QR	GB	HA	NM	VS	WD	YZ	OF	XK	PE	tba	pnc	ukd	nld
St	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	EH	VJ	ZL	PF	nfi	mew	xbk	yes
St	23.	V	II	III	11	21	08	EY	DT	KF	MO	XP	HN	WG	ZL	IV	JA	lsd	nuo	vcr	vcx
St	22.	I	II	IV	01	25	02	PZ	SE	OJ	XF	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nso
St	21.	IV	I	III	06	22	03	GH	JR	TQ	KF	NZ	IL	WM	BD	UO	EC	ema	mlv	jjy	iqh
St	20.	V	I	II	12	25	08	TF	BQ	XV	DZ	PY	NL	WI	SJ	ME	GB	xjl	pgs	ggh	znd
St	19.	IV	III	II	07	05	23	ZX	EU	AC	GD	KP	VO	QS	NW	HL	RM	vpj	zqe	jrs	cgm
St	18.	II	III	V	19	14	22	WG	QM	RL	DB	ST	AQ	PZ	XH	YN	IJ	oxd	lnb	icu	ytt
St	17.	IV	I	II	12	08	21	ME	HX	BP	WY	ZD	TR	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
St	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SG	QU	VJ	YN	EL	pzg	evw	wyt	iye
St	15.	III	II	V	06	16	02	GT	YC	EJ	UA	RX	PN	IS	WB	MH	ZV	bhe	xzm	yzk	evp
St	14.	II	I	V	23	05	24	AZ	CJ	WF	UY	SO	QV	MI	NH	DP	GX	fdx	tyj	bmq	typ
St	13.	IV	II	V	03	25	10	CX	KN	JR	DQ	IU	TL	HZ	MF	EP	WB	zfo	bjr	zwx	gvn
St	12.	I	III	II	26	01	18	QB	YE	WN	AI	GJ	TO	HR	FK	PS	CM	upc	anf	tkr	pwz
St	11.	V	I	III	17	13	04	SV	GO	PA	ZR	FN	HI	YM	WT	DE	BJ	vdh	ego	wmy	uti
St	10.	I	V	IV	26	07	16	SW	AQ	NF	PO	VY	UX	MK	CL	HT	ZJ	rpl	anw	vpr	mhn
St	9.	I	III	IV	17	10	18	EH	IR	GK	NZ	SP	UA	LD	CQ	JM	YV	knq	ysq	rhj	tlj
St	8.	V	II	I	23	11	25	QY	OG	ST	HA	CB	WD	KL	JN	VX	IU	lro	avw	axh	gws
St	7.	II	III	I	06	12	03	BG	FS	TH	JE	VK	PI	CU	QA	OD	NM	aty	mbb	mvo	jmz
St	6.	I	IV	V	24	19	01	IR	HQ	NT	WZ	VC	OY	GP	LF	BX	AK	bhc	iwo	zgz	rnr
St	5.	II	IV	III	05	22	14	MK	GO	RQ	XT	DW	IA	ZL	SY	PJ	EN	bok	rzw	kzo	ryl
St	4.	IV	II	I	15	02	21	KD	PG	CO	FW	HJ	EY	MT	QL	VB	UZ	kpk	php	xmo	pfw
St	3.	III	V	IV	03	23	04	DY	CP	WN	OV	QH	UZ	RA	TI	GL	SM	hjy	nkt	ytn	pvc
St	2.	I	III	V	13	18	01	DR	VJ	PS	EK	IU	HX	AQ	GT	YO	FC	qpq	fqw	oiy	ruj
St	1.	II	IV	I	06	17	26	AC	LS	BQ	WN	MY	UV	FJ	PZ	TR	OK	bol	ooi	ywv	sfb

Enigmas mašīnas 1944. gada dienas uzstādījumi. [14.]

http://www.codesandciphers.org.uk/enigma/enigma3.htm

Enigmas datorsimulāciju un autora programmas SIFRS1, SIFRS2 un SIFRS3 var lejupielādēt šeit - http://failiem.lv/u/blapnvo.

Programmu izpildāmās datnes jāstartē no datora cietā vai noņemamā diska.

2. pielikums

SIFRS3 programmas kods :

```
program sifrs3;
uses crt;
var  burts: char;
     atslega: byte;
     teksts, sifrets: string;
     saglaba, lasa: text;

procedure Nosifre;
var  i, j: byte;
     b, key: char;
begin
   writeln('P- Paraugs');
   writeln('J- Jauns');
   writeln;
   repeat
         key:=upcase(readkey);
         if key='P' then
         begin
              teksts:='dators ir elektroniska ierice datu apstradei';
              writeln('šifrētais paraugteksts ir:');
              writeln(teksts);
         end;
         if key='J' then
         begin
              writeln('Ievadi šifrējamo tekstu mazajiem burtiem:');
              readln(teksts)
         end;
         if (key='P') or (key='J') then
         begin
            randomize;
            atslega:=random(25)+1;
            str(atslega,sifrets);
            for i:=1 to length(teksts) do
            begin
              b:=teksts[i];
              if (b>='a') and (b<='z') then
              for j:=1 to atslega do
              begin
                   b:=succ(b);
                   if b>'z' then b:='a'
              end;
              sifrets:=sifrets+b
            end
         end
   until (key='P') or (key='J')
end;

procedure Atsifre;
var i: byte;
    b: char;
begin
    sifrets:='';
    teksts:='';
    atslega:=0;
    while not eoln(lasa) do
    begin
        read(lasa,b);
        if (b>='0') and (b<='9') then
        begin
           if atslega=0 then atslega:=atslega+ord(b)-48
```

```
              else atslega:=10*atslega+ord(b)-48
         end
         else
         begin
            if sifrets='' then Str(atslega,sifrets);
            sifrets:=sifrets+b;
            if (b>='a') and (b<='z') or (b=' ') then
            begin
                 if b<>' ' then
                 for i:=1 to atslega do
                 begin
                    b:=pred(b);
                    if b<'a' then b:='z'
                 end;
                 teksts:=teksts+b
            end
         end
     end
end;

begin   {----------pamatprogramma------------}

clrscr;
writeln('1- šifrēt  2- Atšifrēt  3- Beigt');
writeln;
repeat
   burts:=readkey;
   if burts='1' then
   begin
      assign(saglaba,'slepens.txt');
      rewrite(saglaba);
      Nosifre;
      writeln(saglaba,sifrets);
      close(saglaba);
      writeln;
      writeln('šifrētais teksts saglabāts kā "slepens.txt"');
      writeln(sifrets);
      writeln
   end;
   if burts='2' then
   begin
         assign(lasa,'slepens.txt');
         {$I-}
         reset(lasa);
         {$I+}
         if IOResult = 0 then
         begin
            Atsifre;
            close(lasa);
            writeln('šifrētais teksts no "slepens.txt" bija:');
            writeln(sifrets);
            writeln;
            writeln('Atšifrētais teksts ir:');
            writeln(teksts)
         end
         else
            writeln('šifrētais teksts no "slepens.txt" neeksistē')
   end
until burts='3'
end.
```