Ruské šifry do r. 1942

O. Grošek

11. 1. 2018

Institute of Computer Science & Mathematics,
Slovak University of Technology,
812 19 Bratislava, Slovakia
otokar.grosek@stuba.sk

Podľa

- (Досья) Татьяна Соболева: Тайнописьв истории России. Москва: Международные отношения, 1994.
- (Досья) Татьяна Соболева: История шифровального дела в России. Москва: ОЛМА–ПРЕСС, 2002. ISBN 5-224-03634-8
- Zdanovič A. A., Izmozik, V. S.: Štyridsať rokov v tajných službách: život a dobrodružstvá Vladimíra Krivoša. – Moskva: Iks-Chistori; Kučkogo pole, 2007. ISBN 978-5-901679-70-8.
- David Kahn: The Codebreakers. - SCRIBINER, 1996
- F.L. Bauer: Decrypted Secrets, Springer - Verlag, 2007
- M. N. Speranskij: Тайнопись в юго-славянских и русских памятниках письма, Энциклопедия славянской филологии, (4) 1929

Úvod

Prehlásenie: Osobne som nerobil žiadny seriózny výskum ruských šifier. Všetko čo uvádzam bolo získané z vyššie uvedených zdrojov, prípadne s vlastným komentárom...

Šifry dávnoveku

Preslav bylo mezi lety 893 - 972 hlavním městem první bulharské říše a jedním z nejdůležitejších středověkých měst v jihovýchodní Evropě. Ruiny města leží asi 20 km jihozápadně od města Šumen. Samo jméno tohoto města poukazuje na rychlou slavonizaci Bulharu. Raně slovanské osídlení bylo na počátku 9. století opevněno a začalo se rychle rozvíjet, hlavně díky blízkosti k původní metropoli Plisce. Nejvetší přínos pro Preslav měla vláda bulharských chánu Kruma a Omurtaga.

- Všetky staré pôvodné rukopisy južných slovanov boli sústredené v Preslavskej škole (Bul.). Tá bolo v r. 970-2 dobitá Kijevským kniežaťom Svjatoslavom a následne Biz. cisárom Jánom I. Knižnica bola prenesená do Kijeva, ktorý bol v polovici 13. st. obsadený Mongolmi a knižnicu spálili... **Takže prvé pamiatky - prepisy - sú až zo XIV. st.**

- Všetky staré pôvodné rukopisy južných slovanov boli sústredené v Preslavskej škole (Bul.). Tá bolo v r. 970-2 dobitá Kijevským kniežaťom Svjatoslavom a následne Biz. cisárom Jánom I. Knižnica bola prenesená do Kijeva, ktorý bol v polovici 13. st. obsadený Mongolmi a knižnicu spálili... **Takže prvé pamiatky - prepisy - sú až zo XIV. st.**
- Okrem toho bolo niečo aj v Srbsku ... Preto sa historici týchto národov hádajú o pôvode textov...

- **Martina Chromá** (UK 2016): *Apokryfní Bartolomějovo evangelium ve slovanské tradici.* Na konci první kapitoly se apoštolové ptají Ježíše, kolik duší za den odejde ze světa, kolik z nich je uznáno spravedlivými a kolik duší se narodí. Podle řecké verze H odejde třicet tisíc duší, podle rkp. G pouze 53 a latinské verze uvádějí konkrétní počty, a sice 6 074 (=2*3037) podle rkp. C a 12 873 (=2*7*613) podle L. Slovanské rukopisy se drží znění podle rkp. H a shodně uvádějí počet 30 000.

- **Martina Chromá** (UK 2016): *Apokryfní Bartolomějovo evangelium ve slovanské tradici.* Na konci první kapitoly se apoštolové ptají Ježíše, kolik duší za den odejde ze světa, kolik z nich je uznáno spravedlivými a kolik duší se narodí. Podle řecké verze H odejde třicet tisíc duší, podle rkp. G pouze 53 a latinské verze uvádějí konkrétní počty, a sice 6 074 (=2*3037) podle rkp. C a 12 873 (=2*7*613) podle L. Slovanské rukopisy se drží znění podle rkp. H a shodně uvádějí počet 30 000.
- Termín *apokryf* je odvodený z gr. s významom *tajný* či *skrytý*. V katolickej a pravoslávnej tradícii sa týmto rozumie spis svojim obsahom a formou podobný starozákonným a novozákonným knihám, ktoré však do biblického kánonu neboli prijaté. (kniha Makabejská, Múdrosti,...)

- **Martina Chromá** (UK 2016): *Apokryfní Bartolomějovo evangelium ve slovanské tradici.* Na konci první kapitoly se apoštolové ptají Ježíše, kolik duší za den odejde ze světa, kolik z nich je uznáno spravedlivými a kolik duší se narodí. Podle řecké verze H odejde třicet tisíc duší, podle rkp. G pouze 53 a latinské verze uvádějí konkrétní počty, a sice 6 074 (=2*3037) podle rkp. C a 12 873 (=2*7*613) podle L. Slovanské rukopisy se drží znění podle rkp. H a shodně uvádějí počet 30 000.
- Termín *apokryf* je odvodený z gr. s významom *tajný* či *skrytý*. V katolickej a pravoslávnej tradícii sa týmto rozumie spis svojim obsahom a formou podobný starozákonným a novozákonným knihám, ktoré však do biblického kánonu neboli prijaté. (kniha Makabejská, Múdrosti,...)
- Mikhail Nestorovich Speranskij (1863—1938) zaviedol pojem Тайнопись.

Niekoľko zaujímavých stránok:

- *http://www.rodon.cz/ikony/Iluminovane-a-vzacne-rukopisy/assemanuv-evangeliar-1681*

Niekoľko zaujímavých stránok:

- *http://www.rodon.cz/ikony/lluminovane-a-vzacne-rukopisy/assemanuv-evangeliar-1681*
- *http://hgr.livejournal.com/1630993.html?thread=25254161*
  Srbská kritika Speranského...

Niekoľko zaujímavých stránok:

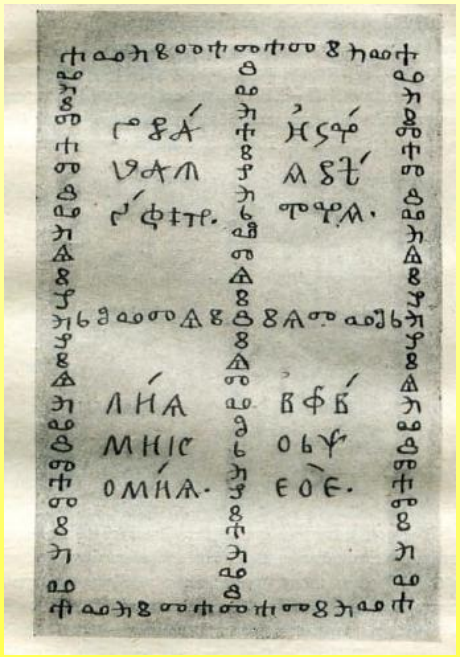
- *http://www.rodon.cz/ikony/Iluminovane-a-vzacne-rukopisy/assemanuv-evangeliar-1681*
- *http://hgr.livejournal.com/1630993.html?thread=25254161*
  Srbská kritika Speranského...
- *https://www.academia.edu/10936379/The_Mysterious_Alphabetum_Iliricum_Sclavorum_*
  The Mysterious " Alphabetum Iliricum Sclavorum"

1. **M. N. Speranskij** v svojom diele opísal množstvo starovekých systémov tajného písma ruských a južných slovanov. Najprv sa len znaky cyriliky (863) nahradzovali znakmi hlaholiky, gréckej abecedy alebo permskej azbuky (episkop Stefan, v XV. st. zanikla), neskôr celé slová, frázy.

1. **M. N. Speranskij** v svojom diele opísal množstvo starovekých systémov tajného písma ruských a južných slovanov. Najprv sa len znaky cyriliky (863) nahradzovali znakmi hlaholiky, gréckej abecedy alebo permskej azbuky (episkop Stefan, v XV. st. zanikla), neskôr celé slová, frázy.
2. Známa je aj "**prostá substitúcia**" kde sa samohlásky nešifrujú a spoluhlásky (20) sa šifrujú ako ATBASH. (1229). (obr. ďalej)

1. **M. N. Speranskij** v svojom diele opísal množstvo starovekých systémov tajného písma ruských a južných slovanov. Najprv sa len znaky cyriliky (863) nahradzovali znakmi hlaholiky, gréckej abecedy alebo permskej azbuky (episkop Stefan, v XV. st. zanikla), neskôr celé slová, frázy.
2. Známa je aj "**prostá substitúcia**" kde sa samohlásky nešifrujú a spoluhlásky (20) sa šifrujú ako ATBASH. (1229). (obr. ďalej)
3. V "**múdrej substitúcii**" sa šifrovali aj samohlásky, znaky boli prebraté z cyriliky. Tiež sa používala **pravouholníkova šifra**, v ktorej sú vynechané niektoré písmená, napr. щ.

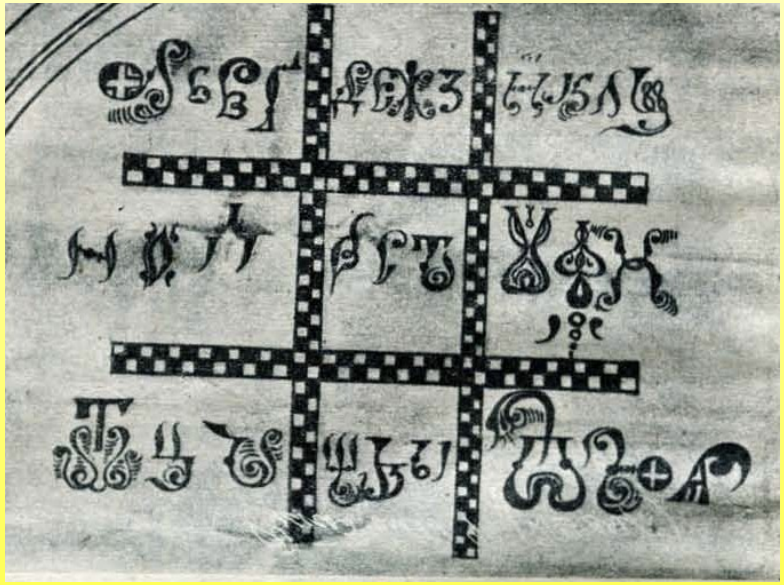
1. **M. N. Speranskij** v svojom diele opísal množstvo starovekých systémov tajného písma ruských a južných slovanov. Najprv sa len znaky cyriliky (863) nahradzovali znakmi hlaholiky, gréckej abecedy alebo permskej azbuky (episkop Stefan, v XV. st. zanikla), neskôr celé slová, frázy.
2. Známa je aj "**prostá substitúcia**" kde sa samohlásky nešifrujú a spoluhlásky (20) sa šifrujú ako ATBASH. (1229). (obr. ďalej)
3. V "**múdrej substitúcii**" sa šifrovali aj samohlásky, znaky boli prebraté z cyriliky. Tiež sa používala **pravouholníkova šifra**, v ktorej sú vynechané niektoré písmená, napr. щ.
4. Je takmer nemožné zistiť, čo sa v skutočnosti používalo do XIII. st. ... lebo všetko sú to len opisy šírené ústnym podaním mníchov...

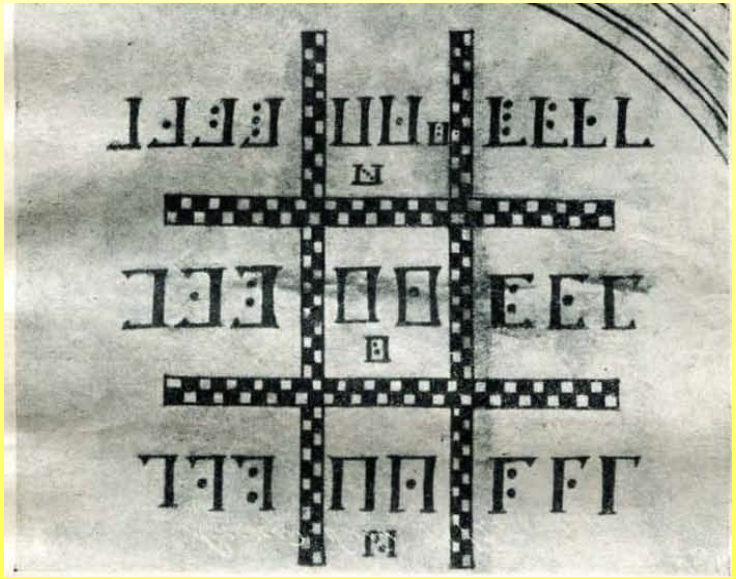


Mních Evstafej (1511) 6 zápisov o jeho práci v hlaholike...

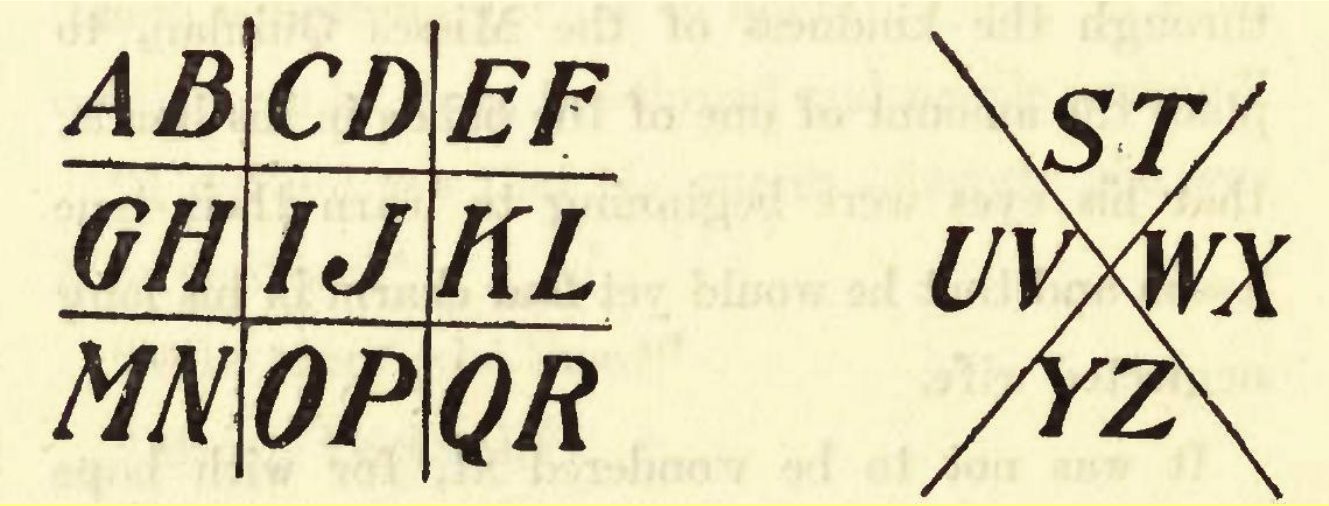
	N	D
I	K	O
I	M	A

XV. st. rukopis zo Sofijskej synody... Tabuľková (nie stĺpcová) transpozícia.





Pravouholíková šifra zo XVII storočia, používaná patriarchami...



Šifra z knihy Anna Katherine Green: The Mayors Wife, 1907
http://ia341336.us.archive.org/1/items/mayorswife00greerich/mayorswife00greerich.pdf

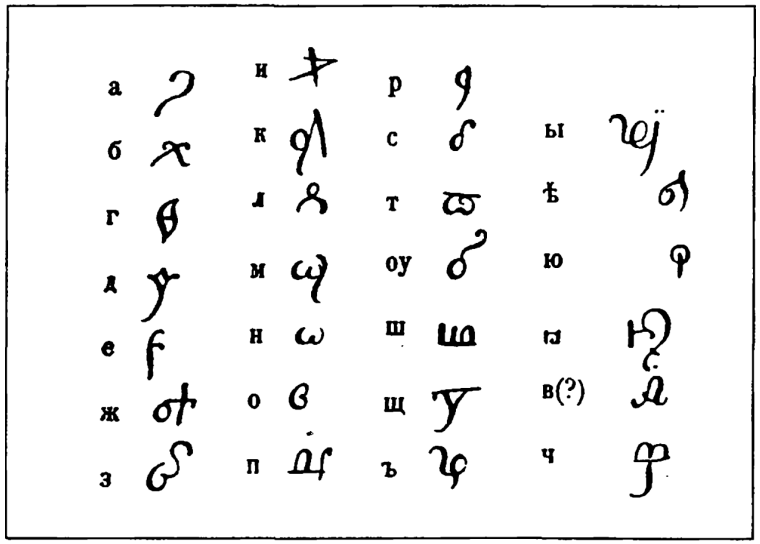
простая литора Bauze prof. na Moskovskej univ. 1229

$C(0, 10) = 945.$

б в г д ж з к л м н

ш щ ч ц ш ф т с р п

N.P. Nikoforov 1590. Deformácia písmen е, л, п, ш, ..., prevrátenie р , grécka abeceda,...



Stredovek

- Počas panovania cára **Fedora Ioannoviča** (1557-1598, syn Ivana Hrozného) už existujú príkazy "písať listy múdrou azbukou", aby okrem cárskeho veličenstva nikto nerozumel (jednoduchá substitúcia).

Stredovek

- Počas panovania cára **Fedora Ioannoviča** (1557-1598, syn Ivana Hrozného) už existujú príkazy "písať listy múdrou azbukou", aby okrem cárskeho veličenstva nikto nerozumel (jednoduchá substitúcia).
- Ruský vyslanec v Gruzínsku K.P. Savin (1597-1598) používal transpozíciu slabík.

Stredovek

- Počas panovania cára **Fedora Ioannoviča** (1557-1598, syn Ivana Hrozného) už existujú príkazy "písať listy múdrou azbukou", aby okrem cárskeho veličenstva nikto nerozumel (jednoduchá substitúcia).
- Ruský vyslanec v Gruzínsku K.P. Savin (1597-1598) používal transpozíciu slabík.
- Za cára **Alekseja Michailoviča** (1629-1676) prišlo k značnému rozšíreniu používania šifier. Napríklad je známe, že keď sa ruský cársky rezident V. M. Tjapkin sťažoval vo Varšave kráľovi Jánovi Sobieckému, že mu meška pošta, kráľ sa na neho oboril, že píše "štvavé a vymyslené listy"...

Stredovek

- Počas panovania cára **Fedora Ioannoviča** (1557-1598, syn Ivana Hrozného) už existujú príkazy "písať listy múdrou azbukou", aby okrem cárskeho veličenstva nikto nerozumel (jednoduchá substitúcia).
- Ruský vyslanec v Gruzínsku K.P. Savin (1597-1598) používal transpozíciu slabík.
- Za cára **Alekseja Michailoviča** (1629-1676) prišlo k značnému rozšíreniu používania šifier. Napríklad je známe, že keď sa ruský cársky rezident V. M. Tjapkin sťažoval vo Varšave kráľovi Jánovi Sobieckému, že mu meška pošta, kráľ sa na neho oboril, že píše "štvavé a vymyslené listy"...
- Na kostoloch sa objavujú texty nesúce znaky steganografie.

Stredovek

- Počas panovania cára **Fedora Ioannoviča** (1557-1598, syn Ivana Hrozného) už existujú príkazy "písať listy múdrou azbukou", aby okrem cárskeho veličenstva nikto nerozumel (jednoduchá substitúcia).
- Ruský vyslanec v Gruzínsku K.P. Savin (1597-1598) používal transpozíciu slabík.
- Za cára **Alekseja Michailoviča** (1629-1676) prišlo k značnému rozšíreniu používania šifier. Napríklad je známe, že keď sa ruský cársky rezident V. M. Tjapkin sťažoval vo Varšave kráľovi Jánovi Sobieckému, že mu meška pošta, kráľ sa na neho oboril, že píše "štvavé a vymyslené listy"...
- Na kostoloch sa objavujú texty nesúce znaky steganografie.
- **Systematické budovanie šifrovej služby** začalo až za cára **Petra Veľkého** (1672-1725) Походная посольская канцелярия, 1702 (Pochodová/cestovná diplomatická kancelária)

Za Petra Veľkého

- Od r. 1709 kancelária centrálne riadila všetku šifrovanú korešpondenciu cára. Prvými vedúcimi boli Gavril Ivanovič Golovkin (1660-1734) a Peter Pavlovič Šafirov (1669-1739), boli to dvaja najvyšší štátny úradníci.

Za Petra Veľkého

- Od r. 1709 kancelária centrálne riadila všetku šifrovanú korešpondenciu cára. Prvými vedúcimi boli Gavril Ivanovič Golovkin (1660-1734) a Peter Pavlovič Šafirov (1669-1739), boli to dvaja najvyšší štátny úradníci.
- OT sa písali v ruštine, francúzštine, nemčine, ale aj gréčtine.

Za Petra Veľkého

- Od r. 1709 kancelária centrálne riadila všetku šifrovanú korešpondenciu cára. Prvými vedúcimi boli Gavril Ivanovič Golovkin (1660-1734) a Peter Pavlovič Šafirov (1669-1739), boli to dvaja najvyšší štátny úradníci.
- OT sa písali v ruštine, francúzštine, nemčine, ale aj gréčtine.
- ZT používala sa cyrilika, latinka, hlaholika, čísla, osobitné znaky, napr. zverokruh, znaky planét,... Napr. znak mesiaca znamenal Mesiac, striebro alebo pondelok, znak ♂Mars, železo, alebo utorok.

Za Petra Veľkého

- Od r. 1709 kancelária centrálne riadila všetku šifrovanú korešpondenciu cára. Prvými vedúcimi boli Gavril Ivanovič Golovkin (1660-1734) a Peter Pavlovič Šafirov (1669-1739), boli to dvaja najvyšší štátny úradníci.
- OT sa písali v ruštine, francúzštine, nemčine, ale aj gréčtine.
- ZT používala sa cyrilika, latinka, hlaholika, čísla, osobitné znaky, napr. zverokruh, znaky planét,... Napr. znak mesiaca znamenal Mesiac, striebro alebo pondelok, znak ♂Mars, železo, alebo utorok.
- Používala sa monoalfabetická a digrafická substitúcia. Tiež sa používali klamače пустышки

Za Petra Veľkého

- Od r. 1709 kancelária centrálne riadila všetku šifrovanú korešpondenciu cára. Prvými vedúcimi boli Gavril Ivanovič Golovkin (1660-1734) a Peter Pavlovič Šafirov (1669-1739), boli to dvaja najvyšší štátny úradníci.
- OT sa písali v ruštine, francúzštine, nemčine, ale aj gréčtine.
- ZT používala sa cyrilika, latinka, hlaholika, čísla, osobitné znaky, napr. zverokruh, znaky planét,... Napr. znak mesiaca znamenal Mesiac, striebro alebo pondelok, znak ♂Mars, železo, alebo utorok.
- Používala sa monoalfabetická a digrafická substitúcia. Tiež sa používali klamače пустышки
- Podľa D. Khana prvá ruská šifra bola zlomená angličanmi v r. 1725.

Príkladom je substitúcia samého "Veľkého vládcu", kde bola pridaná aj malá kódova kniha. Tiež tam boli varianty pre bodku a čiarku. V XVIII. storočí sa tá istá šifra vystriedala pre viacerých používateľov. Zachoval sa list napísaný I. A. Tolstému... “treba odstrániť diakritiku a nedeliť slová...”

А	Б	В	Г	Д	Е	Ж	З	И	К	Л
ме	ли	ко	ин	зе	жу	ню	о	пы	ра	су
М	Н	О	П	Р	С	Т	У	Ф	Х	Ы
ти	у	хи	от	ца	чу	ше	ам	з	ъ	от
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Ъ	Ю	Я	
ь	ъ	ю	я	ф	а	бе	ва	гу	ди	

Очень похожий шифр для переписки И. А. Толстого с князем В. В. Долгоруким сохранился в подлинном письме Петра князю Долгорукому. Копия с этого шифра воспроизведена А. Ф. Бычковым.

- V 30. rokoch sa z nejasných príčin objavujú nové typy šifier - v podstate **kódové knihy**, veľa klamačov a homofónov, špeciálne znaky pre rôznych panovníkov. Napr. nepoužívali sa cifry 3 a 7, ale A=29 sa mohlo písať ak 729, 279, resp. 329, 239, 293.

- V 30. rokoch sa z nejasných príčin objavujú nové typy šifier - v podstate **kódové knihy**, veľa klamačov a homofónov, špeciálne znaky pre rôznych panovníkov. Napr. nepoužívali sa cifry 3 a 7, ale A=29 sa mohlo písať ak 729, 279, resp. 329, 239, 293.
- Iným typom šifry bolo priradenie pre A= 12,13, ...,19,20, 321. Pre B= 21,22,...,28,29,332, Pre C= 30, 31,...,37,38,343.

- V 30. rokoch sa z nejasných príčin objavujú nové typy šifier - v podstate **kódové knihy**, veľa klamačov a homofónov, špeciálne znaky pre rôznych panovníkov. Napr. nepoužívali sa cifry 3 a 7, ale A=29 sa mohlo písať ak 729, 279, resp. 329, 239, 293.
- Iným typom šifry bolo priradenie pre A= 12,13, ...,19,20, 321. Pre B= 21,22,...,28,29,332, Pre C= 30, 31,...,37,38,343.
- Od r. 1744 sa začína objavovať množstvo klamačov, od 165 až po stovky, napr. všetky čísla väčšie ako 3015...

- V 30. rokoch sa z nejasných príčin objavujú nové typy šifier - v podstate **kódové knihy**, veľa klamačov a homofónov, špeciálne znaky pre rôznych panovníkov. Napr. nepoužívali sa cifry 3 a 7, ale A=29 sa mohlo písať ak 729, 279, resp. 329, 239, 293.
- Iným typom šifry bolo priradenie pre A= 12,13, ...,19,20, 321. Pre B= 21,22,...,28,29,332, Pre C= 30, 31,...,37,38,343.
- Od r. 1744 sa začína objavovať množstvo klamačov, od 165 až po stovky, napr. všetky čísla väčšie ako 3015...

Tri substitučné šifry pre korešpondenciu s Haagom od 14.7. 1735 :

1. STUVXYZ - MNOPQR - FGHIKL - ABCDE
2. MNOPQRSTUVXYZ - ABCDEFGHIKL
3. FGHIKL - ABCDE - STUVXYZ - MNOPQR

Založenie Akadémie vied

24.1.1724 vydal Peter I. **príkaz na založenie Akadémie vied.**

Založenie Akadémie vied

24.1.1724 vydal Peter I. **príkaz na založenie Akadémie vied.**

1. Prvé úspechy ruskej kryptoanalýzy sú spojené s menom **Christiana Goldbacha** (1690-1764).

Založenie Akadémie vied

24.1.1724 vydal Peter I. **príkaz na založenie Akadémie vied.**

1. Prvé úspechy ruskej kryptoanalýzy sú spojené s menom **Christiana Goldbacha** (1690-1764).
2. Na pozvanie Petra I. prišli aj - Herman, žiak Jacoba Bernoulliho, Nicola a Daniel - synovia Johana Bernoulliho a neskôr aj Leonard Euler.

Založenie Akadémie vied

24.1.1724 vydal Peter I. **príkaz na založenie Akadémie vied.**

1. Prvé úspechy ruskej kryptoanalýzy sú spojené s menom **Christiana Goldbacha** (1690-1764).
2. Na pozvanie Petra I. prišli aj - Herman, žiak Jacoba Bernoulliho, Nicola a Daniel - synovia Johana Bernoulliho a neskôr aj Leonard Euler.
3. Nie je známe, či sa do dešifrovania zapojil aj Euler, ale Goldbach dosiahol niekoľko vynikajúcich úspechov a aj vďaka nemu koncom XVIII. storočia **ruská dešifrovacia služba dokázala kontrolovať francúzsku diplomatickú poštu**. Napr. dešifroval list FR. ambasadora, v ktorom sa nelichotivo vyjadroval o Petrovej dcére...

Založenie Akadémie vied

24.1.1724 vydal Peter I. **príkaz na založenie Akadémie vied.**

1. Prvé úspechy ruskej kryptoanalýzy sú spojené s menom **Christiana Goldbacha** (1690-1764).
2. Na pozvanie Petra I. prišli aj - Herman, žiak Jacoba Bernoulliho, Nicola a Daniel - synovia Johana Bernoulliho a neskôr aj Leonard Euler.
3. Nie je známe, či sa do dešifrovania zapojil aj Euler, ale Goldbach dosiahol niekoľko vynikajúcich úspechov a aj vďaka nemu koncom XVIII. storočia **ruská dešifrovacia služba dokázala kontrolovať francúzsku diplomatickú poštu**. Napr. dešifroval list FR. ambasadora, v ktorom sa nelichotivo vyjadroval o Petrovej dcére...
4. V r. 1756 sa stal členom akadémie ďalší vynikajúci matematik a fyzik **Franc Ulrich Theodor Epinus** (1724-1802 elektrina a magnetizmus). Zaslúžil sa tiež o prvé kontakty s americkou akadémiou vied.

Za Kataríny

1. Až do konca XVIII. storočia - rozsiahle abecedy 1000-1200 znakov (občas 400-500), ktoré obsahujú okrem abecedy časté bigramy, slová, názvy,..., napr. čísla 5000-5999. Slová sa šifrovali niekedy po písmenách a niekedy ako bigramy.

Za Kataríny

1. Až do konca XVIII. storočia - rozsiahle abecedy 1000-1200 znakov (občas 400-500), ktoré obsahujú okrem abecedy časté bigramy, slová, názvy,..., napr. čísla 5000-5999. Slová sa šifrovali niekedy po písmenách a niekedy ako bigramy.
2. Obsahujú tiež veľké množstvo klamačov, nezriedka 1000, na každom riadku aspoň 3.

Za Kataríny

1. Až do konca XVIII. storočia - rozsiahle abecedy 1000-1200 znakov (občas 400-500), ktoré obsahujú okrem abecedy časté bigramy, slová, názvy,..., napr. čísla 5000-5999. Slová sa šifrovali niekedy po písmenách a niekedy ako bigramy.
2. Obsahujú tiež veľké množstvo klamačov, nezriedka 1000, na každom riadku aspoň 3.
3. Napr. znak + znamenal, že nasledujúci znak možno ignorovať a mal tiež niekoľko ekvivalentov, podobne ++ znamenalo, že nasledujúce dva znaky treba ignorovať,...

Za Kataríny

1. Až do konca XVIII. storočia - rozsiahle abecedy 1000-1200 znakov (občas 400-500), ktoré obsahujú okrem abecedy časté bigramy, slová, názvy,..., napr. čísla 5000-5999. Slová sa šifrovali niekedy po písmenách a niekedy ako bigramy.
2. Obsahujú tiež veľké množstvo klamačov, nezriedka 1000, na každom riadku aspoň 3.
3. Napr. znak + znamenal, že nasledujúci znak možno ignorovať a mal tiež niekoľko ekvivalentov, podobne ++ znamenalo, že nasledujúce dva znaky treba ignorovať,...
4. Podobný význam, ale pre predchádzajúce znaky, mali *, **, ***

Za Kataríny

1. Až do konca XVIII. storočia - rozsiahle abecedy 1000-1200 znakov (občas 400-500), ktoré obsahujú okrem abecedy časté bigramy, slová, názvy,..., napr. čísla 5000-5999. Slová sa šifrovali niekedy po písmenách a niekedy ako bigramy.
2. Obsahujú tiež veľké množstvo klamačov, nezriedka 1000, na každom riadku aspoň 3.
3. Napr. znak + znamenal, že nasledujúci znak možno ignorovať a mal tiež niekoľko ekvivalentov, podobne ++ znamenalo, že nasledujúce dva znaky treba ignorovať,...
4. Podobný význam, ale pre predchádzajúce znaky, mali *, **, ***
5. Znak = znamenal, že treba ignorovať všetky nasledujúce znaky v danom riadku, znak == to isté na danej strane.

Za Kataríny

1. Až do konca XVIII. storočia - rozsiahle abecedy 1000-1200 znakov (občas 400-500), ktoré obsahujú okrem abecedy časté bigramy, slová, názvy,..., napr. čísla 5000-5999. Slová sa šifrovali niekedy po písmenách a niekedy ako bigramy.
2. Obsahujú tiež veľké množstvo klamačov, nezriedka 1000, na každom riadku aspoň 3.
3. Napr. znak + znamenal, že nasledujúci znak možno ignorovať a mal tiež niekoľko ekvivalentov, podobne ++ znamenalo, že nasledujúce dva znaky treba ignorovať,...
4. Podobný význam, ale pre predchádzajúce znaky, mali *, **, ***
5. Znak = znamenal, že treba ignorovať všetky nasledujúce znaky v danom riadku, znak == to isté na danej strane.
6. Znak $\times$ mal tiež 9 ekvivalentov a znamenal, že všetko medzi nimi treba ignorovať.

7 Pred ľubovoľnú štvoricu platných cifier bolo možné napr. písať 5, ktorá nič neznamenala. V iných šifrách sa písalo pred každú trojicu napr. 1...

7 Pred ľubovoľnú štvoricu platných cifier bolo možné napr. písať 5, ktorá nič neznamenala. V iných šifrách sa písalo pred každú trojicu napr. 1...

8 Odporúčalo sa, aby OT bol písaný v dvoch jazykoch Rj a Fr, alebo Rj a Nj. Pri tom odpovedajúce šifrové znaky boli premiešané a nešli za sebou.

7 Pred ľubovoľnú štvoricu platných cifier bolo možné napr. písať 5, ktorá nič neznamenala. V iných šifrách sa písalo pred každú trojicu napr. 1...

8 Odporúčalo sa, aby OT bol písaný v dvoch jazykoch Rj a Fr, alebo Rj a Nj. Pri tom odpovedajúce šifrové znaky boli premiešané a nešli za sebou.

9 Významným počinom bolo, že každý diplomat/špión dostal svoju šifru a tieto sa už neposúvali iným osobám.

7 Pred ľubovoľnú štvoricu platných cifier bolo možné napr. písať 5, ktorá nič neznamenala. V iných šifrách sa písalo pred každú trojicu napr. 1...

8 Odporúčalo sa, aby OT bol písaný v dvoch jazykoch Rj a Fr, alebo Rj a Nj. Pri tom odpovedajúce šifrové znaky boli premiešané a nešli za sebou.

9 Významným počinom bolo, že každý diplomat/špión dostal svoju šifru a tieto sa už neposúvali iným osobám.

10 Napr. fráza Поцелуй ещо раз Александрин znamenala Вам придется покинуть Петербург (1788)

7 Pred ľubovoľnú štvoricu platných cifier bolo možné napr. písať 5, ktorá nič neznamenala. V iných šifrách sa písalo pred každú trojicu napr. 1...

8 Odporúčalo sa, aby OT bol písaný v dvoch jazykoch Rj a Fr, alebo Rj a Nj. Pri tom odpovedajúce šifrové znaky boli premiešané a nešli za sebou.

9 Významným počinom bolo, že každý diplomat/špión dostal svoju šifru a tieto sa už neposúvali iným osobám.

10 Napr. fráza Поцелуй ещо раз Александрин znamenala Вам придется покинуть Петербург (1788)

11 Organizovali sa aj prvé siete - najprv 6 účastníkov, "generálna šifra" len na komunikáciu s jej výsosťou - mala 165 znakov a používalo ju 14 účastníkov (1773), šifra MZV, šifra pre "čierny kabinet",...

7 Pred ľubovoľnú štvoricu platných cifier bolo možné napr. písať 5, ktorá nič neznamenala. V iných šifrách sa písalo pred každú trojicu napr. 1...

8 Odporúčalo sa, aby OT bol písaný v dvoch jazykoch Rj a Fr, alebo Rj a Nj. Pri tom odpovedajúce šifrové znaky boli premiešané a nešli za sebou.

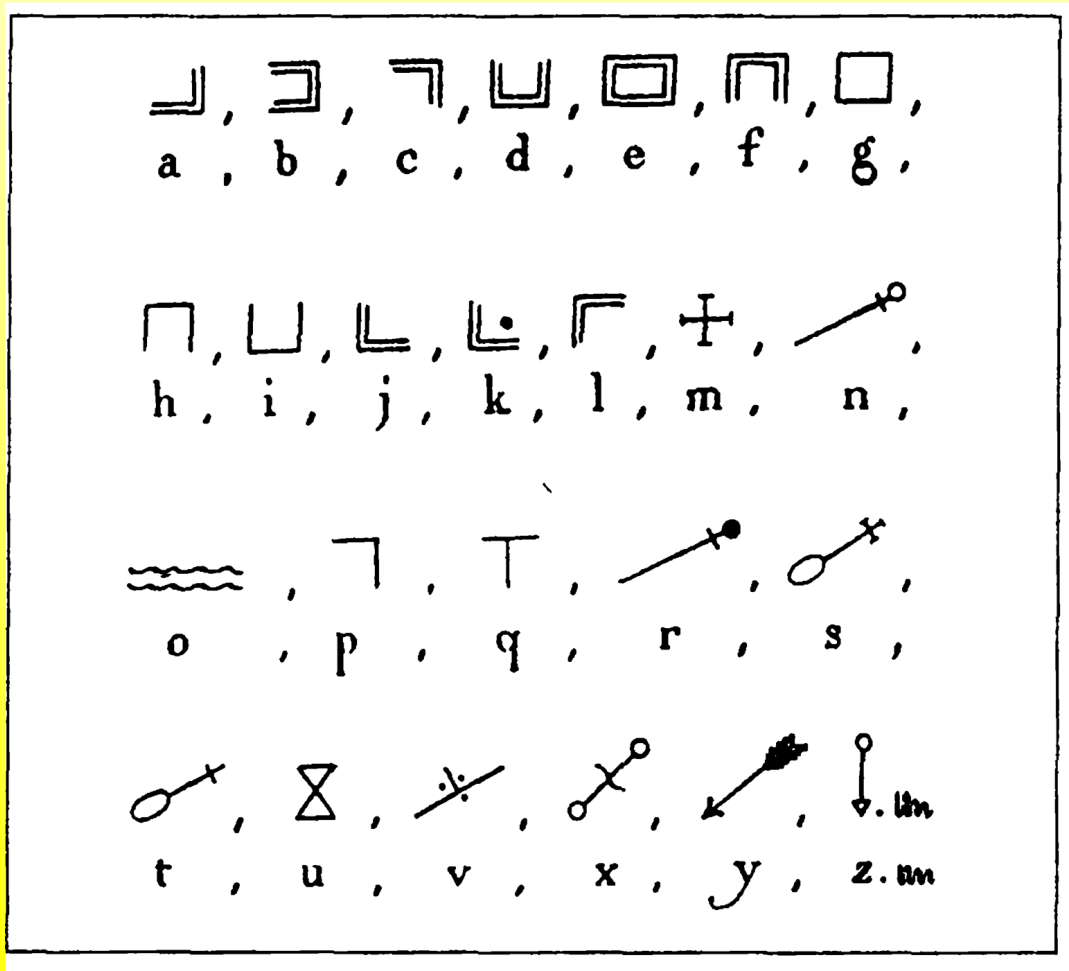
9 Významným počinom bolo, že každý diplomat/špión dostal svoju šifru a tieto sa už neposúvali iným osobám.

10 Napr. fráza Поцелуй ещо раз Александрин znamenala Вам придется покинуть Петербург (1788)

11 Organizovali sa aj prvé siete - najprv 6 účastníkov, "generálna šifra" len na komunikáciu s jej výsosťou - mala 165 znakov a používalo ju 14 účastníkov (1773), šifra MZV, šifra pre "čierny kabinet",...

12 Koncom storočia (26.3.1800) už **ruská rozviedka začína využívať "aktívneho Oscara"** , napr. v korešpondencii pruského kráľa...

Šifra Masonov (slobodomurárov) . Mnohé niesú rozlúštené do dnes. V r. 1790-95 vzrástla cenzúra ich korešpondencie. Išlo o veľmi vzdelaných ľudí s humanitárnou filozofiou... symbolom pripisovali zvláštny význam.



Prvá polovica XIX storočia

1. Cár **Alexander I.** (1801-25, nar. 1777) založil 3 oddelenia - šifrové, kryptoanalitické, a "novinové"(cenzúra vrátane pošty)

Prvá polovica XIX storočia

1. Cár **Alexander I.** (1801-25, nar. 1777) založil 3 oddelenia - šifrové, kryptoanalitické, a "novinové"(cenzúra vrátane pošty)
2. Rozširovali sa siete šifrovanej komunikácie.

barón Pavel Ľvovič Schilling (1786-1837)

1. Elektrický telegraf 21. 10. 1832 v Petrohrade (100m) a 1835 na kongrese v Bone (5km) (6 r. skôr ako bezdrôtový Popov, Morze a Murgaš 1838).

barón Pavel Ľvovič Schilling (1786-1837)

1. Elektrický telegraf 21. 10. 1832 v Petrohrade (100m) a 1835 na kongrese v Bone (5km) (6 r. skôr ako bezdrôtový Popov, Morze a Murgaš 1838).
2. Princíp - vychyľovanie kompasu pri vodiči s el. prúdom. Vymyslel 6 znakový telegrafný kód - slová váhy 1-3, tj. spolu 41. Jeden znak bola zmena, takže celkove mala abeceda OT 81 znakov.

barón Pavel Ľvovič Schilling (1786-1837)

1. Elektrický telegraf 21. 10. 1832 v Petrohrade (100m) a 1835 na kongrese v Bone (5km) (6 r. skôr ako bezdrôtový Popov, Morze a Murgaš 1838).
2. Princíp - vychyľovanie kompasu pri vodiči s el. prúdom. Vymyslel 6 znakový telegrafný kód - slová váhy 1-3, tj. spolu 41. Jeden znak bola zmena, takže celkove mala abeceda OT 81 znakov.
3. Zaviedol bigramové šifrovanie Fr. jazyka pričom **bigramy OT sa tvorili zo znakov s periódou** T (nezávislosť, dĺžka textu $2T$). Ak už neboli znaky, prešlo sa na jednoduchú substitúciu, alebo sa vytvoril padding.

Druhá polovica XIX storočia a začiatok XX.

Bigramové šifry sa začali masovo využívať v rôznych oblastiach záujmu Ruska. Bola vykonaná reforma abecedy a znížil sa počet základných znakov, aby sa to ľahšie prenášalo cez telegraf. Počet bigramov bol 1296, preto sa šifrovalo pomocou 1,2 a 4 gramov.

Biklave

- Vytvorí sa 24 pások, na každej páske je 5 štvoríc znakov z TSA s opakovaním, každá páska je označená písmenom z TSA. Napr. **W: qduf kziv akil swkm pzcq**. Pásky sa menili 1 krát za rok.

Biklave

- Vytvorí sa 24 pások, na každej páske je 5 štvoríc znakov z TSA s opakovaním, každá páska je označená písmenom z TSA. Napr. **W: qduf kziv akil swkm pzcq**. Pásky sa menili 1 krát za rok.
- OT sa napíše nad W:

zajt	ra-s	auiv	dime	zase
qduf	kziv	akil	swkm	pzcq

Biklave

- Vytvorí sa 24 pások, na každej páske je 5 štvoríc znakov z TSA s opakovaním, každá páska je označená písmenom z TSA. Napr. **W: qduf kziv akil swkm pzcq**. Pásky sa menili 1 krát za rok.
- OT sa napíše nad W:

zajt	ra-s	auiv	dime	zase
qduf	kziv	akil	swkm	pzcq

- Tak dostávame dvojice (z,q), (a,d),... Existuje tabuľka 26×26, ktorá má riadky označené 23 znakmi (bez k,w,y) a navyše znaky -, . Stĺpce sú označené TSA. V každom stĺpci je ľubovoľných 17 znakov TSA a cifry 1-9 bez opakovania.

Šifrovnie

- Na prvých 20 znakov sa použije napr. páska W (jedna z 24) (riadok, stĺpec) = (z,q) zodpovedá v tabuľke napr. j = ZT. atď.

Šifrovnie

- Na prvých 20 znakov sa použije napr. páska W (jedna z 24) (riadok, stĺpec) = (z,q) zodpovedá v tabuľke napr. j = ZT. atď.
- Pri dešifrovaní je to naopak (q,j) = z.

Šifrovnie

- Na prvých 20 znakov sa použije napr. páska W (jedna z 24) (riadok, stĺpec) = (z,q) zodpovedá v tabuľke napr. j = ZT. atď.
- Pri dešifrovaní je to naopak (q,j) = z.
- Pri šifrovaní správy sa mohlo použiť najviac 8 pások. Ak šifrujeme viac ako 20×8 znakov, procedúra sa opakuje.

Šifrovnie

- Na prvých 20 znakov sa použije napr. páska W (jedna z 24) (riadok, stĺpec) = (z,q) zodpovedá v tabuľke napr. j = ZT. atď.
- Pri dešifrovaní je to naopak (q,j) = z.
- Pri šifrovaní správy sa mohlo použiť najviac 8 pások. Ak šifrujeme viac ako 20×8 znakov, procedúra sa opakuje.
- V OT k sa píše ako qq, w ako vv, y ako ii, ; ako ., atď.

Šifrovnie

- Na prvých 20 znakov sa použije napr. páska W (jedna z 24) (riadok, stĺpec) = (z,q) zodpovedá v tabuľke napr. j = ZT. atď.
- Pri dešifrovaní je to naopak (q,j) = z.
- Pri šifrovaní správy sa mohlo použiť najviac 8 pások. Ak šifrujeme viac ako 20×8 znakov, procedúra sa opakuje.
- V OT k sa píše ako qq, w ako vv, y ako ii, ; ako ., atď.
- Ak poznáme tabuľku a poradie pások nepoznáme, tak skúšame ich poradie. Na prvú pásku je 24 možností, na druhú 23,..., na ôsmu 17, spolu 164 možností

Šifrovacie kódy

- Jazyk obsahuje 7000 - 8000 najpoužívanejších slov, ale napr. vo vojenstve stačí okolo 1000 slov. Argentiovci požívali 1200 slov - 1586.

Šifrovacie kódy

- Jazyk obsahuje 7000 - 8000 najpoužívanejších slov, ale napr. vo vojenstve stačí okolo 1000 slov. Argentiovci požívali 1200 slov - 1586.
- Prešifrovanie malo názvy gréckej abecedy $\alpha, \beta, \gamma, \ldots$ Napr. γ je vlastne Vernamova šifra. Kód + γ sa používal aj v 50. - 60 rokoch XX. storočia.

Šifrovacie kódy

- Jazyk obsahuje 7000 - 8000 najpoužívanejších slov, ale napr. vo vojenstve stačí okolo 1000 slov. Argentiovci požívali 1200 slov - 1586.
- Prešifrovanie malo názvy gréckej abecedy $\alpha, \beta, \gamma, \ldots$ Napr. γ je vlastne Vernamova šifra. Kód + γ sa používal aj v 50. - 60 rokoch XX. storočia.
- Používala sa aj šifra stĺpcovej transpozície, kľúče boli v 2 knihách, každá 667 strán... Bola aj pomôcka $\mathrm{Скала}$, vojaci požívali aj zámenu poradia cifier v ZT.

Ministerstvo vojny používalo na prešifrovanie známu šifru (1910) označenú ako B

- Zjednodušená ruská abeceda má 30 znakov, tabuľka 30×30 , každý riadok je permutácia, prvý riadok aj stĺpec v základnom tvare. Každý znak OT sa zobrazí na 2 znaky ZT. Iná verzia boli zlomky riadok/ stĺpec...

Ministerstvo vojny používalo na prešifrovanie známu šifru (1910) označenú ako B

- Zjednodušená ruská abeceda má 30 znakov, tabuľka 30×30 , každý riadok je permutácia, prvý riadok aj stĺpec v základnom tvare. Každý znak OT sa zobrazí na 2 znaky ZT. Iná verzia boli zlomky riadok/ stĺpec...
- Periodické heslo malo dĺžku minimálne 10 znakov. To sa použilo ako perióda vo Vigenere....

Ministerstvo vojny používalo na prešifrovanie známu šifru (1910) označenú ako B

- Zjednodušená ruská abeceda má 30 znakov, tabuľka 30×30 , každý riadok je permutácia, prvý riadok aj stĺpec v základnom tvare. Každý znak OT sa zobrazí na 2 znaky ZT. Iná verzia boli zlomky riadok/ stĺpec...
- Periodické heslo malo dĺžku minimálne 10 znakov. To sa použilo ako perióda vo Vigenere....Jednoduchá expanzná tabuľka 6×6 priradí znaku azbuky dvojicu cifier 1-6. OT sa prepíše do číselnej podoby, zvolí sa kľúč - fráza prepísaná rovnakým spôsobom. Potom sa sčituje bez modulu. Výsledok môže byť niekedy aj trojmiestny...

Ministerstvo vojny používalo na prešifrovanie známu šifru (1910) označenú ako B

- Zjednodušená ruská abeceda má 30 znakov, tabuľka 30×30 , každý riadok je permutácia, prvý riadok aj stĺpec v základnom tvare. Každý znak OT sa zobrazí na 2 znaky ZT. Iná verzia boli zlomky riadok/ stĺpec...
- Periodické heslo malo dĺžku minimálne 10 znakov. To sa použilo ako perióda vo Vigenere....Jednoduchá expanzná tabuľka 6×6 priradí znaku azbuky dvojicu cifier 1-6. OT sa prepíše do číselnej podoby, zvolí sa kľúč - fráza prepísaná rovnakým spôsobom. Potom sa sčituje bez modulu. Výsledok môže byť niekedy aj trojmiestny...
- Policajná šifra používala 30 substitúcií, každý znak sa šifroval dvojicou (číslo perm., ZT)...

Ministerstvo vojny používalo na prešifrovanie známu šifru (1910) označenú ako B

- Zjednodušená ruská abeceda má 30 znakov, tabuľka 30×30 , každý riadok je permutácia, prvý riadok aj stĺpec v základnom tvare. Každý znak OT sa zobrazí na 2 znaky ZT. Iná verzia boli zlomky riadok/ stĺpec...
- Periodické heslo malo dĺžku minimálne 10 znakov. To sa použilo ako perióda vo Vigenere....Jednoduchá expanzná tabuľka 6×6 priradí znaku azbuky dvojicu cifier 1-6. OT sa prepíše do číselnej podoby, zvolí sa kľúč - fráza prepísaná rovnakým spôsobom. Potom sa sčituje bez modulu. Výsledok môže byť niekedy aj trojmiestny...
- Policajná šifra používala 30 substitúcií, každý znak sa šifroval dvojicou (číslo perm., ZT)...

- V XIX. a prvej polovici XX. storočia ešte agenti používali jednoduché a dvojité transpozície. Za zmienku stojí, že rozmery tabuľky sa dajú zisťovať aj pomocou najčastejších bigramov, v Rj. CT, MC. Preto sa text z tabuliek čítal inak ako po stĺpcoch...

- V XIX. a prvej polovici XX. storočia ešte agenti používali jednoduché a dvojité transpozície. Za zmienku stojí, že rozmery tabuľky sa dajú zisťovať aj pomocou najčastejších bigramov, v Rj. CT, MC. Preto sa text z tabuliek čítal inak ako po stĺpcoch...
- Používal sa P-kód podobne ako vo VIC šifre...

	3	9	4	6	1	0	8	5	7	2
	U	Z		T	O		V	I	E	M
4	A	B	C	D	F	G	H	J	K	L
0	N	P	Q	R	S	W	X	Y		

- V XIX. a prvej polovici XX. storočia ešte agenti používali jednoduché a dvojité transpozície. Za zmienku stojí, že rozmery tabuľky sa dajú zisťovať aj pomocou najčastejších bigramov, v Rj. CT, MC. Preto sa text z tabuliek čítal inak ako po stĺpcoch...
- Používal sa P-kód podobne ako vo VIC šifre...

	3	9	4	6	1	0	8	5	7	2
	U	Z		T	O		V	I	E	M
4	A	B	C	D	F	G	H	J	K	L
0	N	P	Q	R	S	W	X	Y		

- Bela Kun (1886 – 1938) posielal do Moskvy takto šifrované správy v r. 1919 a američania to vedeli čítať...
- V r. 1934 bol v Kodani zadržaný šifrovací disk, ktorý používali dánsky komunisti na komunikáciu s Moskvou... Išlo o verziu disku Argentiovcov z XVI. st. Kahn sa vo svojej knihe pýtal, či o tom ateistický komunisti vedeli...

- V XIX. a prvej polovici XX. storočia ešte agenti používali jednoduché a dvojité transpozície. Za zmienku stojí, že rozmery tabuľky sa dajú zisťovať aj pomocou najčastejších bigramov, v Rj. CT, MC. Preto sa text z tabuliek čítal inak ako po stĺpcoch...
- Používal sa P-kód podobne ako vo VIC šifre...

	3	9	4	6	1	0	8	5	7	2
	U	Z		T	O		V	I	E	M
4	A	B	C	D	F	G	H	J	K	L
0	N	P	Q	R	S	W	X	Y		

- Bela Kun (1886 – 1938) posielal do Moskvy takto šifrované správy v r. 1919 a američania to vedeli čítať...
- V r. 1934 bol v Kodani zadržaný šifrovací disk, ktorý používali dánsky komunisti na komunikáciu s Moskvou... Išlo o verziu disku Argentiovcov z XVI. st. Kahn sa vo svojej knihe pýtal, či o tom ateistický komunisti vedeli...

Začiatok XX. storočia

Na scéne sa objavuje **Vladimír Ivanovič Krivoš - Nemanič**...

Počas Rusko - Japonskej vojny (1904-5) pracoval v gen. štábe.
Rozlúštil 3 japonské kľúče (z 5), jeden rozlúštili Fr (boli spojenci)
Odcestoval do Paríža a spolu rozlúštili aj posledný.

- Na prelome st. sa začal využívať telegraf, čo malo veľký vplyv aj na šifrovanie - možnosť odpočúvania. Začali sa prijímať telegrafisti, rádiotechnici, lingvisti a matematici.

- Na prelome st. sa začal využívať telegraf, čo malo veľký vplyv aj na šifrovanie - možnosť odpočúvania. Začali sa prijímať telegrafisti, rádiotechnici, lingvisti a matematici.
- Na **Ruskom vyslanectve v Pekingu** (1888) došlo ku veľkej krádeži kľúčov. Podobne v Port Arthure 1904-5. **To prispelo ku porážke Rusov v tejto vojne. Krivoš písal, že mal len 2-3 spolupracovníkov, ktorí vedeli o čo ide pri šifrovaní...**

- Na prelome st. sa začal využívať telegraf, čo malo veľký vplyv aj na šifrovanie - možnosť odpočúvania. Začali sa prijímať telegrafisti, rádiotechnici, lingvisti a matematici.
- Na **Ruskom vyslanectve v Pekingu** (1888) došlo ku veľkej krádeži kľúčov. Podobne v Port Arthure 1904-5. **To prispelo ku porážke Rusov v tejto vojne. Krivoš písal, že mal len 2-3 spolupracovníkov, ktorí vedeli o čo ide pri šifrovaní...**
- Rusi na začiatku WW1 1913-4 rozlúštili 2939 šifier (569 Rak., 171 Nem., 246 Bulh., 181 Tur.,..) **Vo Viedni bol veľký trh..**

- Na prelome st. sa začal využívať telegraf, čo malo veľký vplyv aj na šifrovanie - možnosť odpočúvania. Začali sa prijímať telegrafisti, rádiotechnici, lingvisti a matematici.
- Na **Ruskom vyslanectve v Pekingu** (1888) došlo ku veľkej krádeži kľúčov. Podobne v Port Arthure 1904-5. **To prispelo ku porážke Rusov v tejto vojne. Krivoš písal, že mal len 2-3 spolupracovníkov, ktorí vedeli o čo ide pri šifrovaní...**
- Rusi na začiatku WW1 1913-4 rozlúštili 2939 šifier (569 Rak., 171 Nem., 246 Bulh., 181 Tur.,..) **Vo Viedni bol veľký trh..**
- **Alfred Redl** (1864 - 1913) bol plukovník rakúsko-uhorskej armády a velitel generálneho štábu VIII. zboru (Praha) a špión. Vo svojej predošlej kariére pracoval zväčša v riadiacej pozícii rakúsko-uhorskej vojenskej služby Evidenzbureau (Evidenčná kancelária). Kvôli jeho homosexualite bol vydierateľný, čo využila ruská tajná služba, ktorá ho naverbovala ako špióna. Stal sa najdôležitejším špiónom cárskeho Ruska a v r. 1902 predal Rusku kódovu knihu Rakúska. Ku koncu kariéry poskytoval tajné dokumenty aj talianskej a francúzskej tajnej službe. Spáchal samovraždu.

Šifry ruských revolucionárov

1. Jedn. substitúcia daná 1-2 frázami, abeceda mala 34 znakov.

Šifry ruských revolucionárov

1. Jedn. substitúcia daná 1-2 frázami, abeceda mala 34 znakov.
2. Často používaná "štvorcová šifra" 1-9,0. V prvom stĺpci je fráza

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

AGENT = 21, 27, 24, 14, 33 = 30, 27, 24, 51, 56 = ...

3 Zložitý štvorec - poradie stĺpcov sa zmení 10 znakovou frázou...

3 Zložitý štvorec - poradie stĺpcov sa zmení 10 znakovou frázou...

4 Vynechá sa napr. 4 a 7 riadok/stĺpec a tam sa píše čokoľvek

3. Zložitý štvorec - poradie stĺpcov sa zmení 10 znakovou frázou...
4. Vynechá sa napr. 4 a 7 riadok/stĺpec a tam sa píše čokoľvek
5. множественный квадрат niekoľko štvorcov, ktoré sa striedajú...

3. Zložitý štvorec - poradie stĺpcov sa zmení 10 znakovou frázou...
4. Vynechá sa napr. 4 a 7 riadok/stĺpec a tam sa píše čokoľvek
5. множественный квадрат niekoľko štvorcov, ktoré sa striedajú...
6. Klasický **Vigenere, ale bez modulu**, existovali aj varianty, že sa sčitovalo po cifrách...

3. Zložitý štvorec - poradie stĺpcov sa zmení 10 znakovou frázou...
4. Vynechá sa napr. 4 a 7 riadok/stĺpec a tam sa píše čokoľvek
5. множественный квадрат niekoľko štvorcov, ktoré sa striedajú...
6. Klasický **Vigenere, ale bez modulu**, existovali aj varianty, že sa sčitovalo po cifrách...
7. V časopise **ISKRA** (šéfredaktor **N. Krupskaja**) sa 20.10.1901 písalo, ako používať šifry... *neoddelovať slová, neopakovať často rovnaké znaky pre časté písmená, písať tak, aby sa nedala určiť šifra, nepoužívať známe básne z kníh...*

Šifry opozície - občianska vojna

Hráči 1918 - 22/23

1. červenoarmejci - prívrženci Lenina, bolševici, ...
2. bielogvardejci - zvyšky cárskej armády, šifru riadil B. Savinkov, štvorec 10×10 a 10×30,...
3. Kolčakovci - neúspechy bielych viedli ku odovzdaniu velenia admirálovi Kolčakovi. Keď ho opustili eseri, začal prehrávať...
4. anarchisti, ukrajinská armáda,...
5. intervenčné vojská Francúzske, Polské, Legionári,...

1. **Kolčak** si ponechal cárskych šifrantov - mali navrch... Používali kódové knihy až 8000 znakov, substitučné, transpozičné,..., **autokľúč OT s posunutými znakmi o** $h = 1$; prvé písmeno bolo dohodnuté. Je to ekvivalentné s Vigenére s periodickým kľúčom (k,-k), takže stačí vyskúšať 26 znakov...Všeobecne:

1. **Kolčak** si ponechal cárskych šifrantov - mali navrch... Používali kódové knihy až 8000 znakov, substitučné, transpozičné,..., **autokľúč OT s posunutými znakmi o** $h = 1$; prvé písmeno bolo dohodnuté. Je to ekvivalentné s Vigenére s periodickým kľúčom (k,-k), takže stačí vyskúšať 26 znakov...Všeobecne:

2. $$y_i = \begin{cases} x_i + k_i \bmod 26, & \text{for } i = 0, 1, \ldots, r-1; \\ x_i + x_{i-r} + h, & \text{for } i \geq r. \end{cases}$$

1. **Kolčak** si ponechal cárskych šifrantov - mali navrch... Používali kódové knihy až 8000 znakov, substitučné, transpozičné,..., **autokľúč OT s posunutými znakmi o** $h = 1$; prvé písmeno bolo dohodnuté. Je to ekvivalentné s Vigenére s periodickým kľúčom (k,-k), takže stačí vyskúšať 26 znakov...Všeobecne:

2. $$y_i = \begin{cases} x_i + k_i \bmod 26, & \text{for } i = 0, 1, \ldots, r-1; \\ x_i + x_{i-r} + h, & \text{for } i \geq r. \end{cases}$$

3. $$y_n = x_n + (-1)^{\lfloor n/r \rfloor} k_{n \bmod r} + D(n, r) + h(\lfloor n/r \rfloor \bmod 2),$$

   kde

$$D(n, r) = \sum_{i=1}^{\lfloor n/r \rfloor} (-1)^{i+1} y_{n-ir}.$$

4 Takže z daného ZT y_i sa vytvorí nový ZT Y_i šifry Vigenere s kľúčom $(k_0, k_1, \ldots, k_{r-1})$ ...

4. Takže z daného ZT y_i sa vytvorí nový ZT Y_i šifry Vigenere s kľúčom $(k_0, k_1, \ldots, k_{r-1})$ ...
5. Vedeli čítať všetky šifry červených... Na príkaz Lenina sa začala budovať nová šifrovacia služba. 12. 4. 1921 predstavil **Gleb Ivanovič Bokij** svoj plán. Boli stanovené rôzne úlohy:

4. Takže z daného ZT y_i sa vytvorí nový ZT Y_i šifry Vigenere s kľúčom $(k_0, k_1, \ldots, k_{r-1})$ ...
5. Vedeli čítať všetky šifry červených... Na príkaz Lenina sa začala budovať nová šifrovacia služba. 12. 4. 1921 predstavil **Gleb Ivanovič Bokij** svoj plán. Boli stanovené rôzne úlohy:
   - vo vedeckej oblasti analýza starých a tvorba nových, zozbieranie archívnych materiálov, príručky, ...
   - vytvorenie nových šifier - porovnanie so súčasným stavom, inštrukcie na ich používanie
   - organizácia výučby - program, založenie školy, nábor učiteľov
   - orgány a ich organizácia....

4. Takže z daného ZT y_i sa vytvorí nový ZT Y_i šifry Vigenere s kľúčom $(k_0, k_1, \ldots, k_{r-1})$ ...
5. Vedeli čítať všetky šifry červených... Na príkaz Lenina sa začala budovať nová šifrovacia služba. 12. 4. 1921 predstavil **Gleb Ivanovič Bokij** svoj plán. Boli stanovené rôzne úlohy:
   - vo vedeckej oblasti analýza starých a tvorba nových, zozbieranie archívnych materiálov, príručky, ...
   - vytvorenie nových šifier - porovnanie so súčasným stavom, inštrukcie na ich používanie
   - organizácia výučby - program, založenie školy, nábor učiteľov
   - orgány a ich organizácia....
6. **Bokij zavolal do služby aj Krivoša...** a v r. 1933 už mali 100 ľudí a 89 v zahraničí.

- Začali s naštudovaním znalosti dorevolučného Ruska (dešifrovanie tureckých, perzských japonských a iných...)

- Začali s naštudovaním znalosti dorevolučného Ruska (dešifrovanie tureckých, perzských japonských a iných...)
- Študovali aj "originály" šifier USA, Nemecka, Japonska, Číny, Bulharska, ako aj zahraničných učebníc.

- Začali s naštudovaním znalosti dorevolučného Ruska (dešifrovanie tureckých, perzských japonských a iných...)
- Študovali aj "originály" šifier USA, Nemecka, Japonska, Číny, Bulharska, ako aj zahraničných učebníc.
- **Najväčšiu úlohu zohrali I.A. Zybin a V.I. Krivoš - Nemanič...**

- Začali s naštudovaním znalosti dorevolučného Ruska (dešifrovanie tureckých, perzských japonských a iných...)
- Študovali aj "originály" šifier USA, Nemecka, Japonska, Číny, Bulharska, ako aj zahraničných učebníc.
- **Najväčšiu úlohu zohrali I.A. Zybin a V.I. Krivoš - Nemanič...**
- Organizovali 6 mesačné kurzy ...

- Koncom r. 1919 **Herbert Yardley dešifroval sovietsku agentúrnu šifru vertikálnej transpozície** - nerovnaké dĺžky stĺpcov. Mal k dispozícii veľké množstvo dát od pilota nemeckého lietadla, ktoré pristálo v Lotyšsku.

- Koncom r. 1919 **Herbert Yardley dešifroval sovietsku agentúrnu šifru vertikálnej transpozície** - nerovnaké dĺžky stĺpcov. Mal k dispozícii veľké množstvo dát od pilota nemeckého lietadla, ktoré pristálo v Lotyšsku.
- Podľa neho Rusko a Japonsko boli jediné krajiny, čo používali kódové slová nerovnakej dĺžky, Rusko ich používalo ešte v 30. rokoch...

- Koncom r. 1919 **Herbert Yardley dešifroval sovietsku agentúrnu šifru vertikálnej transpozície** - nerovnaké dĺžky stĺpcov. Mal k dispozícii veľké množstvo dát od pilota nemeckého lietadla, ktoré pristálo v Lotyšsku.
- Podľa neho Rusko a Japonsko boli jediné krajiny, čo používali kódové slová nerovnakej dĺžky, Rusko ich používalo ešte v 30. rokoch...
- Od r. 1921 **Rusi vedeli čítať všetky diplomatické kódy Nemecka a Turecka, od r. 1924 Poľský kód, spolu od r. 1925 kódy 15 štátov.**

- Koncom r. 1919 **Herbert Yardley dešifroval sovietsku agentúrnu šifru vertikálnej transpozície** - nerovnaké dĺžky stĺpcov. Mal k dispozícii veľké množstvo dát od pilota nemeckého lietadla, ktoré pristálo v Lotyšsku.
- Podľa neho Rusko a Japonsko boli jediné krajiny, čo používali kódové slová nerovnakej dĺžky, Rusko ich používalo ešte v 30. rokoch...
- Od r. 1921 **Rusi vedeli čítať všetky diplomatické kódy Nemecka a Turecka, od r. 1924 Poľský kód, spolu od r. 1925 kódy 15 štátov.**
- od r. 1927 Japonský, od r. 1930 niektoré kódy USA.

Šifrové oddelenie Červenej armády

- 28.3. 1928 bolo rozhodnuté o zriadení šifrového odd. a v auguste 1930 už pracovalo pod vedení, Ja. K. Berzina, 46 ľudí.

Šifrové oddelenie Červenej armády

- 28.3. 1928 bolo rozhodnuté o zriadení šifrového odd. a v auguste 1930 už pracovalo pod vedení, Ja. K. Berzina, 46 ľudí.
- Spísal požiadavky na pracovníka "..., vyššie vzdelanie, aspoň jeden cudzí jazyk, schopnosť samostatnej vedecko - výskumnej práce, široká vedecká erudícia, trpezlivosť, kombinatorické schopnosti".

Šifrové oddelenie Červenej armády

- 28.3. 1928 bolo rozhodnuté o zriadení šifrového odd. a v auguste 1930 už pracovalo pod vedení, Ja. K. Berzina, 46 ľudí.
- Spísal požiadavky na pracovníka "..., vyššie vzdelanie, aspoň jeden cudzí jazyk, schopnosť samostatnej vedecko - výskumnej práce, široká vedecká erudícia, trpezlivosť, kombinatorické schopnosti".
- Neustále sa vzdelávať v kryptografii. "Takí pracovníci sa vychovajú za veľa rokov a výsledky sa dostavujú až po viacročných skúsenostiach na špeciálnom pracovisku..."

Šifrové oddelenie Červenej armády

- 28.3. 1928 bolo rozhodnuté o zriadení šifrového odd. a v auguste 1930 už pracovalo pod vedení, Ja. K. Berzina, 46 ľudí.
- Spísal požiadavky na pracovníka "..., vyššie vzdelanie, aspoň jeden cudzí jazyk, schopnosť samostatnej vedecko - výskumnej práce, široká vedecká erudícia, trpezlivosť, kombinatorické schopnosti".
- Neustále sa vzdelávať v kryptografii. "Takí pracovníci sa vychovajú za veľa rokov a výsledky sa dostavujú až po viacročných skúsenostiach na špeciálnom pracovisku..."
- V r. 1929 ušiel G.S. Agabekov, I. Rejss, A. Barmin a gen. V. Krivickij - všetci tvrdili, že v ZSSR je "kontrarevolúcia"(Stalin) a "Kainovia robotníckej triedy ... ničia dielo revolúcie".

Stalinské čistky

- v r. 1989 žurnál "Sobesednik", a potom "Pravda" uverejnili životopis predvojnového rozviedčíka Dmitija Alexandroviča Bysholetova, ktorý bol najprv 11 r. agentom v zahraničí, a potom 16 r. v stalinských gulagoch...

Stalinské čistky

- v r. 1989 žurnál "Sobesednik", a potom "Pravda" uverejnili životopis predvojnového rozviedčíka Dmitija Alexandroviča Bysholetova, ktorý bol najprv 11 r. agentom v zahraničí, a potom 16 r. v stalinských gulagoch...
- SLON - "Soloveckij Lager Osobovo Naznačenia", na výstavbe participoval aj Bokij a Ejchmans... (6 r. tam bol aj Krivoš...)

Stalinské čistky

- v r. 1989 žurnál "Sobesednik", a potom "Pravda" uverejnili životopis predvojnového rozviedčíka Dmitija Alexandroviča Bysholetova, ktorý bol najprv 11 r. agentom v zahraničí, a potom 16 r. v stalinských gulagoch...
- SLON - "Soloveckij Lager Osobovo Naznačenia", na výstavbe participoval aj Bokij a Ejchmans... (6 r. tam bol aj Krivoš...)
- 7.7. 1937 boli zavretí ako "slobodomurári" a v októbri 1937 ich zastrelili spolu s ďaľšími 40 kryptológmi vrátane Guseva...

Stalinské čistky

- v r. 1989 žurnál "Sobesednik", a potom "Pravda" uverejnili životopis predvojnového rozviedčíka Dmitija Alexandroviča Bysholetova, ktorý bol najprv 11 r. agentom v zahraničí, a potom 16 r. v stalinských gulagoch...
- SLON - "Soloveckij Lager Osobovo Naznačenia", na výstavbe participoval aj Bokij a Ejchmans... (6 r. tam bol aj Krivoš...)
- 7.7. 1937 boli zavretí ako "slobodomurári" a v októbri 1937 ich zastrelili spolu s ďaľšími 40 kryptológmi vrátane Guseva...
- Šifrová služba bola oslabená a musela sa spojiť civilná a armádna služba... Od r. 1939 mala armáda opäť svoju službu.

Stalinské čistky

- v r. 1989 žurnál "Sobesednik", a potom "Pravda" uverejnili životopis predvojnového rozviedčíka Dmitija Alexandroviča Bysholetova, ktorý bol najprv 11 r. agentom v zahraničí, a potom 16 r. v stalinských gulagoch...
- SLON - "Soloveckij Lager Osobovo Naznačenia", na výstavbe participoval aj Bokij a Ejchmans... (6 r. tam bol aj Krivoš...)
- 7.7. 1937 boli zavretí ako "slobodomurári" a v októbri 1937 ich zastrelili spolu s ďaľšími 40 kryptológmi vrátane Guseva...
- Šifrová služba bola oslabená a musela sa spojiť civilná a armádna služba... Od r. 1939 mala armáda opäť svoju službu.
- V r. 1941 prišla do služby z Moskovskej univerzity skupina CSc z M, F a technických vied...

Stalinské čistky

- v r. 1989 žurnál "Sobesednik", a potom "Pravda" uverejnili životopis predvojnového rozviedčíka Dmitija Alexandroviča Bysholetova, ktorý bol najprv 11 r. agentom v zahraničí, a potom 16 r. v stalinských gulagoch...
- SLON - "Soloveckij Lager Osobovo Naznačenia", na výstavbe participoval aj Bokij a Ejchmans... (6 r. tam bol aj Krivoš...)
- 7.7. 1937 boli zavretí ako "slobodomurári" a v októbri 1937 ich zastrelili spolu s ďaľšími 40 kryptológmi vrátane Guseva...
- Šifrová služba bola oslabená a musela sa spojiť civilná a armádna služba... Od r. 1939 mala armáda opäť svoju službu.
- V r. 1941 prišla do služby z Moskovskej univerzity skupina CSc z M, F a technických vied...
- Niekedy v r. 1942/43 získali sovieti ENIGMU aj s kódovou knihou, ale uložili to do skladu...

- V tom čase Japonci pozývali zahr. vedcov, napr. Jána Kowalewského, člena FR AV, pôvodom z Polska. Vyučil Razibara Ita a Kvišio Naksuki. Ito rozlúštil PlayFair...

- V tom čase Japonci pozývali zahr. vedcov, napr. Jána Kowalewského, člena FR AV, pôvodom z Polska. Vyučil Razibara Ita a Kvišio Naksuki. Ito rozlúštil PlayFair...
- V r. 1949 z rozhodnutia najvyšších miest - na Mat. inštitúte Steklova AN ZSSR vytvorili odd. aplikovaných štúdií (riadil ho Vinogradov - šifry...) a odd. Aplikovanej matematiky (riadil ho Keldyš - kozmos). Boli tam napr. A.A. Markov, Linnik, Fadejev...

- V tom čase Japonci pozývali zahr. vedcov, napr. Jána Kowalewského, člena FR AV, pôvodom z Polska. Vyučil Razibara Ita a Kvišio Naksuki. Ito rozlúštil PlayFair...
- V r. 1949 z rozhodnutia najvyšších miest - na Mat. inštitúte Steklova AN ZSSR vytvorili odd. aplikovaných štúdií (riadil ho Vinogradov - šifry...) a odd. Aplikovanej matematiky (riadil ho Keldyš - kozmos). Boli tam napr. A.A. Markov, Linnik, Fadejev... Malcev a Šafarevič sa z toho vyzuli, že nebudú pracovať pre KGB...

- Russian copulation - správa rozdelená na dve približne rovnaké časti a poslané jedna za druhou bez hlavičky...

- Russian copulation - správa rozdelená na dve približne rovnaké časti a poslané jedna za druhou bez hlavičky...
- V Rusku vytvárali v 40. rokoch XX. náhodné postupnosti sekretárky...ľavá/pravá ruka...

- Russian copulation - správa rozdelená na dve približne rovnaké časti a poslané jedna za druhou bez hlavičky...
- V Rusku vytvárali v 40. rokoch XX. náhodné postupnosti sekretárky...ľavá/pravá ruka...
- Sovieti vedeli lúštiť NATO šifrátor KW-7. Od konca r. 1941 vedeli lúštiť japonský šifrátor PURPLE...

Zhrnutie podľa (Dosie) Svetlany Soboleva

- Všetko sa začalo Petrom Veľkým... aktívne využívanie klamačov, viac jazykov, špeciálne postupy, ktoré komplikovali dešifrovanie...

Zhrnutie podľa (Dosie) Svetlany Soboleva

- Všetko sa začalo Petrom Veľkým... aktívne využívanie klamačov, viac jazykov, špeciálne postupy, ktoré komplikovali dešifrovanie...
- 1742 založenie dešifrovacej služby, zachytávanie správ, vedecký základ - Goldbach, Epimus a i. Významné úspechy pri dešifrovaní Fr., Ang. a Nem. šifier

Zhrnutie podľa (Dosie) Svetlany Soboleva

- Všetko sa začalo Petrom Veľkým... aktívne využívanie klamačov, viac jazykov, špeciálne postupy, ktoré komplikovali dešifrovanie...
- 1742 založenie dešifrovacej služby, zachytávanie správ, vedecký základ - Goldbach, Epimus a i. Významné úspechy pri dešifrovaní Fr., Ang. a Nem. šifier
- V tom čase boli rovnocenní s Fr., Ang. a Tal. Objavili sa rôzne pomôcky, tabuľky na uľahčenie práce. Zaostávali v organizácii a výchove kádrov, vedeckej práce a publikovaní výsledkov...

Zhrnutie podľa (Dosie) Svetlany Soboleva

- Všetko sa začalo Petrom Veľkým... aktívne využívanie klamačov, viac jazykov, špeciálne postupy, ktoré komplikovali dešifrovanie...
- 1742 založenie dešifrovacej služby, zachytávanie správ, vedecký základ - Goldbach, Epimus a i. Významné úspechy pri dešifrovaní Fr., Ang. a Nem. šifier
- V tom čase boli rovnocenní s Fr., Ang. a Tal. Objavili sa rôzne pomôcky, tabuľky na uľahčenie práce. Zaostávali v organizácii a výchove kádrov, vedeckej práce a publikovaní výsledkov...
- Knihy Kassiského 1863 a Kerckhoffa 1883 nepoužívali...

Zhrnutie podľa (Dosie) Svetlany Soboleva

- Všetko sa začalo Petrom Veľkým... aktívne využívanie klamačov, viac jazykov, špeciálne postupy, ktoré komplikovali dešifrovanie...
- 1742 založenie dešifrovacej služby, zachytávanie správ, vedecký základ - Goldbach, Epimus a i. Významné úspechy pri dešifrovaní Fr., Ang. a Nem. šifier
- V tom čase boli rovnocenní s Fr., Ang. a Tal. Objavili sa rôzne pomôcky, tabuľky na uľahčenie práce. Zaostávali v organizácii a výchove kádrov, vedeckej práce a publikovaní výsledkov...
- Knihy Kassiského 1863 a Kerckhoffa 1883 nepoužívali...
- V XIX. a zač. XX. st. sa kryptografii nevenoval žiaden matematik. Schilling bol výnimkou, ale to bol elektroinžinier...

- Vo vojenských akadémiach vo svete sa od r. 1881 učila kryptografia (Krivoš vo Viedni), ale v Rusku nie.

- Vo vojenských akadémiach vo svete sa od r. 1881 učila kryptografia (Krivoš vo Viedni), ale v Rusku nie.
- Nezaostávali vo využití kódov a ich prešifrovaní, poznali knihu Bazeriho 1901 ako lúštiť kódy bez prešifrovania.

- Vo vojenských akadémiach vo svete sa od r. 1881 učila kryptografia (Krivoš vo Viedni), ale v Rusku nie.
- Nezaostávali vo využití kódov a ich prešifrovaní, poznali knihu Bazeriho 1901 ako lúštiť kódy bez prešifrovania.
- Počas WW1 a revolúcie zaostávali, neboli žiadne úspechy, iba prehry...

- Vo vojenských akadémiach vo svete sa od r. 1881 učila kryptografia (Krivoš vo Viedni), ale v Rusku nie.
- Nezaostávali vo využití kódov a ich prešifrovaní, poznali knihu Bazeriho 1901 ako lúštiť kódy bez prešifrovania.
- Počas WW1 a revolúcie zaostávali, neboli žiadne úspechy, iba prehry...
- V období občianskej vojny mali bielogvardejci navrch a v 20. rokoch zaostávali za západom. Kryptografia nebola veda ale "pole pôsobnosti"...

- Vo vojenských akadémiach vo svete sa od r. 1881 učila kryptografia (Krivoš vo Viedni), ale v Rusku nie.
- Nezaostávali vo využití kódov a ich prešifrovaní, poznali knihu Bazeriho 1901 ako lúštiť kódy bez prešifrovania.
- Počas WW1 a revolúcie zaostávali, neboli žiadne úspechy, iba prehry...
- V období občianskej vojny mali bielogvardejci navrch a v 20. rokoch zaostávali za západom. Kryptografia nebola veda ale "pole pôsobnosti"...
- 20. - 30. roky boli úpadkom, na konci 30. rokov sa postupne začali využívať analytické a syntetické metódy, M, F a Ch.

Doslov

- V úvode autorka píše, že motívom napísania knihy bolo jej osobné stretnutie s D. Kahnom, ktorý vo svojej knihy píše veľmi nelichotivo o ruskej kryptografii, a doslovne píše ..."čo možno očakávať od ruských mužíkov..."Ten jej povedal nech napíše svoju vlastnú verziu...(D. Kahn - kap. 18 Русская Криптология 614-671)

Doslov

- V úvode autorka píše, že motívom napísania knihy bolo jej osobné stretnutie s D. Kahnom, ktorý vo svojej knihy píše veľmi nelichotivo o ruskej kryptografii, a doslovne píše ..."čo možno očakávať od ruských mužíkov..."Ten jej povedal nech napíše svoju vlastnú verziu...(D. Kahn - kap. 18 Русская Криптология 614-671)
- Na konci knihy sa čitateľ dozvie, že autorka pracovala na 8. veliteľstve KGB... a v Kahnovej knihe, že prvá "manželka" Krivošovho syna sa volala Досья...

Doslov

- V úvode autorka píše, že motívom napísania knihy bolo jej osobné stretnutie s D. Kahnom, ktorý vo svojej knihy píše veľmi nelichotivo o ruskej kryptografii, a doslovne píše ..."čo možno očakávať od ruských mužíkov..."Ten jej povedal nech napíše svoju vlastnú verziu...(D. Kahn - kap. 18 Русская Криптология 614-671)
- Na konci knihy sa čitateľ dozvie, že autorka pracovala na 8. veliteľstve KGB... a v Kahnovej knihe, že prvá "manželka" Krivošovho syna sa volala Досья...
- Na ospravedlnenie autorka píše: "Zatiaľ čo nemci pálili knihy *cudzích*, v ZSSR sa pálili knihy *vlastných* ...

Doslov

- V úvode autorka píše, že motívom napísania knihy bolo jej osobné stretnutie s D. Kahnom, ktorý vo svojej knihy píše veľmi nelichotivo o ruskej kryptografii, a doslovne píše ..."čo možno očakávať od ruských mužíkov..."Ten jej povedal nech napíše svoju vlastnú verziu...(D. Kahn - kap. 18 Русская Криптология 614-671)
- Na konci knihy sa čitateľ dozvie, že autorka pracovala na 8. veliteľstve KGB... a v Kahnovej knihe, že prvá "manželka" Krivošovho syna sa volala Дося...
- Na ospravedlnenie autorka píše: "Zatiaľ čo nemci pálili knihy *cudzích*, v ZSSR sa pálili knihy *vlastných* ...
- Kahn veľmi kritizuje Bokého, že rád pil a "ženy sa ho báli..." Autorka podáva svoj vlastný opis, opisuje jeho štúdium, ako bol populárny v spoločnosti, vedel krásne spievať a hrať na gitare - proste kto by mu odolal...

Doslov

- V úvode autorka píše, že motívom napísania knihy bolo jej osobné stretnutie s D. Kahnom, ktorý vo svojej knihy píše veľmi nelichotivo o ruskej kryptografii, a doslovne píše ..."čo možno očakávať od ruských mužíkov..."Ten jej povedal nech napíše svoju vlastnú verziu...(D. Kahn - kap. 18 Русская Криптология 614-671)
- Na konci knihy sa čitateľ dozvie, že autorka pracovala na 8. veliteľstve KGB... a v Kahnovej knihe, že prvá "manželka" Krivošovho syna sa volala Дося...
- Na ospravedlnenie autorka píše: "Zatiaľ čo nemci pálili knihy *cudzích*, v ZSSR sa pálili knihy *vlastných* ...
- Kahn veľmi kritizuje Bokého, že rád pil a "ženy sa ho báli..." Autorka podáva svoj vlastný opis, opisuje jeho štúdium, ako bol populárny v spoločnosti, vedel krásne spievať a hrať na gitare - proste kto by mu odolal...

- Tiež nesúhlasí s Kahnom, že používali len Cézarovu šifru... Píše ako akýsi Kolenin, pracovník šifrovej služby kritizoval v liste stav šifry na začiatku WW I a jeho kritiku sa pokúšali uviesť do života (proste nezastrelili ho...)

- Tiež nesúhlasí s Kahnom, že používali len Cézarovu šifru... Píše ako akýsi Kolenin, pracovník šifrovej služby kritizoval v liste stav šifry na začiatku WW I a jeho kritiku sa pokúšali uviesť do života (proste nezastrelili ho...)
- Kahn čerpal len zo správ zahraničných služieb opisujúcich neúspechy, ale na druhej strane je veľmi presný. Zatiaľ čo autorka popisuje všeky udalosti väčšinou bez detailov, a skôr vymenúva zoznamy pracovísk a pracovníkov...

- Tiež nesúhlasí s Kahnom, že používali len Cézarovu šifru... Píše ako akýsi Kolenin, pracovník šifrovej služby kritizoval v liste stav šifry na začiatku WW I a jeho kritiku sa pokúšali uviesť do života (proste nezastrelili ho...)
- Kahn čerpal len zo správ zahraničných služieb opisujúcich neúspechy, ale na druhej strane je veľmi presný. Zatiaľ čo autorka popisuje všeky udalosti väčšinou bez detailov, a skôr vymenúva zoznamy pracovísk a pracovníkov...
- KONIEC

Klávesnica:
0. ‘,1,2,3,4,5,6,7,8,9,0,-,ı

1. ч,щ,е,р,т,ы,у,и,о,п,[,]

2. а,с,д,ф,г,х,j,к,л,;,’,

3. з,ш,ц,в,б,н,м

4. й, ё, ь, ъ, э, Э
alebo
ђ, ж, ль, нь, х, ц, ч, ш, щ, ю, я,