INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Demonstrátor KEYMAKER

Název: **Rekonstrukce šifrovacího stroje ŠD-2**

Vypracoval: **Vojtěch Brtník**

Datum: **30. 11. 2009**

Tato práce vznikla za podpory projektu MŠMT CZ.1.07/2.3.00/09.0067 TeamIT – Budování konkurenceschopných výzkumných týmů pro IT.

Rekonstrukce šifrovacího stroje ŠD-2

Vojtěch Brtník, MFF UK Praha (vojtech@brtnik.eu)

Historie stroje

Bezpečnostní situace menších států, tedy i Československa byla vždy komplikovaná. V období nástupu rotorových šifrátorů se již vědělo, že kryptografie je doménou matematiků. Od roku 1945 do roku 1955 se na československém ministerstvu obrany postupně pracovalo na vývoji nejméně devíti typů šifrátorů. Žádný ale nebyl použit v armádním ani jiném provozu, neboť již tehdy prováděné kryptoanalýzy neměly zcela kladné výsledky. Místo toho byly používány např. zahraniční trofejní stroje.

V roce 1955 vznikla Zvláštní správa Ministerstva vnitra, která měla mimo jiné i gesci na vývoj a testování kryptografických prostředků. V roce 1957 byla vládou ČSR požádána sovětská strana o pomoc při výrobě šifrátoru. Sovětská strana vyhověla a počátkem listopadu 1957 dodala do Československa k testování dva kusy stroje, které měly představovat vzor pro výrobu šifrátoru s označením ŠD-2. Jednalo se o modifikaci ruského šifrátoru CM-I.

Nicméně situace se zdála být komplikovanou. Problémy s domácí výrobou, zejména časová zdlouhavost, náročnost s přepracováním technické a výrobní dokumentace, utajení vlastní výroby, vyškolení techniků a organizování celého procesu se ukázalo jako příliš velká překážka. Druhou možností byla sériová výroba strojů v SSSR. Tato varianta by vyřešila mnoho komplikací domácí výroby a taktéž by zkrátila dobu čekání na nový šifrátor. Zádrhelem této varianty byla ale příliš velká cena jednoho stroje, a tak ani k její realizaci nedošlo. ŠD-2 nebyl v Československu nakonec nikdy dále vyvíjen, či nasazen do praxe a je tak v našich dějinách již pouze historickým odkazem.

Popis stroje

ŠD-2 byl elektromechanický diskový šifrátor s vlastní tvorbou hesla určený pro šifrování offline. Elektrické impulsy zajišťovaly přenos elektrického kontaktu od vstupního zařízení skrz šifrátor k výstupnímu zařízení. Mechanika pak zajišťovala vše ostatní, tedy otáčení a posouvání jednotlivých částí stroje, funkčnost klávesnice i tiskacího a perforačního zařízení. Kromě obyčejného tisku na papír umí také děrovat písmena do dálnopisné (perforační) pásky pomocí pětimístného Baudotova kódu. Také vstup bylo možné zadat buď ručně z klávesnice, nebo automaticky pomocí dálnopisné pásky.

Šifrátor měří 511 × 514 × 282 milimetrů a váží 41,5 kilogramů. Kostru tvoří již zmíněná klávesnice, snímač dálnopisné perforační pásky, tiskací a dálnopisné děrovací (perforační) zařízení. Součástí je dále podstavec, hnací jednotka a šifrovací blok.

Hnací jednotka se skládá z elektromotoru, převodních hřídelů, mechanických zařízení na počítání pracovních cyklů stroje a posouvání pracovních součástek. Je to mechanické srdce stroje, zajímavé hlavně ze strojařského pohledu. Elektromotor byl schopen pracovat jak na střídavý proud s napětím v rozmezí od 100V do 230V, tak na stejnosměrný proud s napětím 110V.

Šifrovací jednotka

Vlastní šifrovací jednotka se skládá z 26 elektromagnetických obvodů. Ty se v každém kroku šifrátoru mění a tvoří pro každý pracovní cyklus unikátní substituční šifru.

Elektromagnetický obvod začíná na konci klávesnicové páky nebo po načtení vstupního písmene na perforační pásce, dále pokračuje do přepínače druhu práce, kde se rozhodne, jestli proud šifrovým blokem půjde po směru (šifrování), proti směru (dešifrování), nebo se celý šifrovací blok přeskočí a vstup se rovnou vytiskne (režim psacího stroje).

Při šifrování se z přepínače druhu práce postupuje do kolíkového komutátoru, pravého pevného disku, pěti vnitřních pracovních disků, levého pevného disku až k výstupnímu zařízení. Při dešifrování se postupuje opačně.

Kolíkový komutátor

Kolíkový komutátor je určen pro změnu spojení šifrovacích obvodů při vchodu do šifrátoru. Je umístěn mimo vlastní šifrovací blok na lehce dostupném místě a umožňuje tak jednoduchým způsobem bez nutnosti cokoliv rozebírat změnit počáteční nastavení šifrovacích obvodů.

Skládá se ze dvou skupin zdířek, pracovně nazvaných VSTUP a VÝSTUP, každá skupina je rozdělena do dvou řad po 13 písmenech (A-M, N-Z). Zdířky skupiny VSTUP jsou pak spojeny vodiči se zdířkami skupiny výstup dle denního klíče. Těmito vodiči pak putuje vlastní elektrický impuls při šifrování/dešifrování. Při šifrování ve směru VSTUP > VÝSTUP, při dešifrování naopak. Zdířky skupiny VSTUP jsou spojeny s přepínačem druhu práce, zdířky skupiny VÝSTUP s pravým pevným diskem.

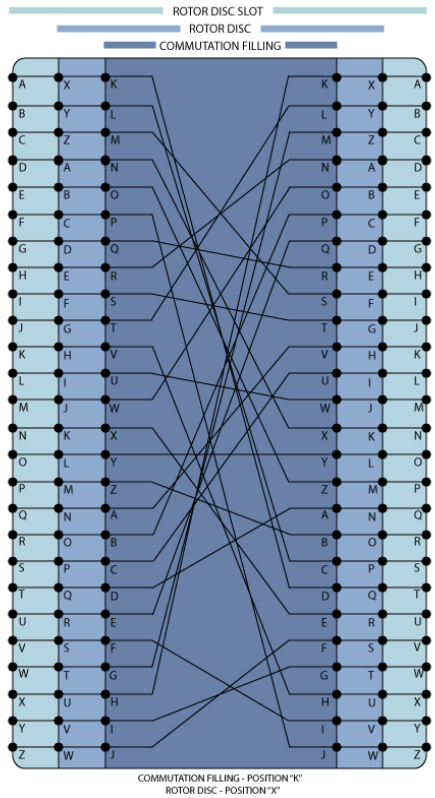
Pravý pevný disk

Také nazýván vstupní pevný disk. Slouží pouze k převodu elektrického impulsu na ostatní šifrové disky. Z hlediska bezpečnosti nemá žádnou funkci.

Vnitřní pracovní disky

Vnitřní pracovní disky jsou srdcem šifrátoru a z hlediska bezpečnosti to nejpodstatnější. Vnitřních šifrových disků je pět, označených čísly 1 – 5. Pořadí, v jakém se poskládají za sebe na osu, je dáno denním klíčem. Každý pevný disk má na obou svých stranách 26 elektrických zakončení, kterými probíhá elektrický impuls. Pracovní disk se v každém kroku stroje, tj. po zpracování jednoho písmene, otáčí o určitý počet pozic, konkrétně o 0-2 pozice a mění tak zapojení elektrických obvodů. Uvnitř disku je komutační vložka. Ta je vlastním nositelem šifrové informace. V disku je ustanovena v jedné z 26 pevných pozic, ta je dána denní klíčovou tabulkou stejně jako výběr kompletu šifrových vložek.

Schéma zapojení jednoho pracovního disku je znázorněno na obrázku.



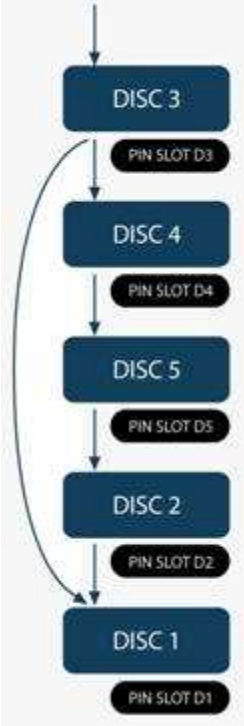
Černými čarami je vyznačeno 26 elektrických vodičů tvořících 26 elektrických obvodů. Tmavě modrou barvou je naznačena komutační vložka, světlejší je pak vlastní disk. Ten se v každém kroku otáčí a otáčí také komutační vložkou, která je v něm vložena. Jednotlivá písmena na obvodu komutační vložky i pevného disku jsou pouze pro obsluhu stroje, aby mohla jednodušeji nastavit stroj do počáteční polohy. Nejsvětlejší modrou barvou je pak vyznačen pouze abstraktní prostor, v kterém se pracovní disk pohybuje. Poskládáme-li pět těchto abstraktních prostorů za sebe do sekvence a sledujeme-li jednu z čar od začátku až do konce, získáme, které písmeno otevřeného textu se zašifruje na které (samozřejmě: ignorujeme nyní přítomnost kolíkového komutátoru a pevných disků na krajích).

Levý pevný disk

Také nazýván výstupní pevný disk. Na rozdíl od pravého pevného disku i on slouží jako nositel bezpečností informace. Je v něm vložena komutační vložka. Levý pevný disk se nikdy netočí. Můžeme si jej proto představit stejně jako kolíkový komutátor na druhém konci posloupností šifrových jednotek. Jen je o dost obtížnější změnit jeho zapojení, protože abychom vyměnili komutační vložku uvnitř, musíme disk celý rozebrat.
Která komutační vložka a v jaké poloze v něm bude ustanovena, je opět dáno denním klíčem. Ten bude popsán níže.

Rotování pracovních disků

Jak již bylo řečeno, tak v každém kroku stroje se pět pracovních disků otočí o určitý počet pozic a změní tak v dalším kroku používanou substituční šifru. O kolik se jednotlivé disky pootočí, udávají kolíčky, které se vkládají do jednotlivých disků na některé z 26 pracovních pozic. Podle jakého klíče jsou kolíčky do disků umisťovány, není známo. Pravděpodobně jde o dlouhodobý směnný prvek, který je určen pro celou skupinu strojů komunikujících spolu. Teoreticky může být umístěno 0 – 26*5 kolíčků. Kolíčky v disku 1 ale nehrají žádnou roli.
V každém kroku každého disku je pak aktivní jedna z pozic a podle toho, zdali se v ní nachází kolíček nebo ne, se disk pootočí o určitý počet zubů.



Postupně se otáčejí jednotlivé disky. Je-li otočen jeden disk, tak ve směru šipek je přesunuta otáčivá síla na vedlejší disk. Síla se přesune pouze v tom případě, že v daném místě není zablokována kolíčkem. Tedy disk 3 se otočí vždy o 1 pozici, disk 1 minimálně o 1, maximálně o 2, zbytek stojí nebo se otočí o 1. Z obrázku je také patrné, že kolíčky v disku 1 nehrají žádnou roli, protože již nemají co blokovat.

Příklad. Představme si, že kolíček je pouze u disku 4. Otočí se tedy disk 3, přenese sílu na disk 4 a disk 1. Disk 4 chce přenést sílu na disk 5, ale tomu zabrání kolíček. Z disku 1 už není kam sílu přenést, a tedy se otočí disky 3, 4 a 1 o jednu pozici, disky 5 a 2 se nehýbou. Za zmínku také stojí, že v tomto případě je naprosto irelevantní, zdali je v aktivní pozici disku 5 či disku 2 kolíček.

Popis klíče a režimů komunikace

Stroj pracuje ve třech režimech komunikace: vzájemné, oběžníkové a obecné. K nastavení stroje je potřeba znát denní a jednorázový klíč. Denní klíč je společný pro všechny režimy komunikace, jednorázový se liší v závislosti na daném režimu. Dlouhodobým směnným prvkem je dále již diskutované umístění kolíčků v jednotlivých discích.

Denní klíč

Každá pracovní stanice disponovala denní klíčovou tabulku. Ta byla distribuovaná pravděpodobně měsíčně a byla společná pro celou komunikační síť. Denní klíč se skládá z následujících položek:

- Určení dne v měsíci, pro který daný klíč platí
- Výběr šesti komutačních vložek (z kompletu 26) a určení strany, kterou bude komutační vložka do daného disku vložena
- Úhlové natočení komutačních vložek v discích
- Pořadí šifrových disků na ose šifrovacího bloku
- Zapojení kolíkového komutátoru

Jeden záznam v tabulce denních klíčů vypadal například takto:

02
AXFPRH XZSSDF 13542
ABCDEFGHIJKLMNOPQRSTUVWXYZ
PKLSFZTBXCYQMADGEJHIORNUWV

Obsluha stroje použije tento klíč druhý den v měsíci, pro který je daná klíčová tabulka distribuována a bude postupovat následovně:

- Z kompletu 26 komutačních vložek budou vybrány vložky A, X, F, P, R a H. Vložka A bude vložena do levého pevného disku. Vložky X, F, P, R a H pak postupně zleva do prvního až pátého vnitřního pracovního disku. Vložka A, P a H bude vložena lícem, zbylé rubem. Komutační vložky mají pro tyto účely od výroby vyražené písmeno, na lícové straně bez potržení, na rubové s podtržením

- Disky budou na osu vloženy v pořadí 1-3-5-4-2, přičemž disk 1 bude úplně vlevo, disky mají pro tyto účely od výroby vyražené číslo.

- V komutátoru bude písmeno A skupiny VSTUP spojeno s písmenem P skupiny VÝSTUP, písmeno B s písmenem K, až písmeno Z s písmenem V.

Vzájemná komunikace

Vzájemná komunikace sloužila pro výhradní komunikaci dvou stran. Každá ze dvou komunikujících stran měla k dispozici tabulku jednorázových klíčů. Ta byla stejná pro obě

strany a musela být distribuovaná před samotnou komunikací. Ve vzájemném režimu komunikace tak mohly komunikovat pouze dvojice, jež byly předem ustaveny, a byla jim distribuována tabulka jednorázových klíčů.

Na začátku každé zašifrované zprávy bylo otevřeně odesláno číslo řádku, jehož jednorázový klíč se má použít. Vlastní jednorázový klíč sestává z pětice písmen a udává úhlové natočení vnitřních pracovních disků před vlastním šifrováním. Jako první disk je uveden disk levý.

Formát zprávy v režimu vzájemné komunikace
Na začátek se otevřeným textem napsal příjemce, důležitost zprávy a další případně podstatné informace, dále se uvedl řádek v tabulce jednorázových klíčů. Poté se tímto jednorázovým klíčem zašifrovala vlastní zpráva. Nakonec se opět otevřeným textem uvedla takzvaná služební skupina, a to den odeslání zprávy, které tak určilo denní klíč a počet pětiznakových skupin v dané zprávě.

Zpráva připravená k odeslání dálnopisem tedy mohla vypadat například takto:

125 DULEZITE 02 ACKSD KDLSIE LDKFHD LDIEZC LDKEIF LKXXX **02008**

Tato zpráva byla odeslána 2. dne v měsíci adresátovi s číslem 125 s poznámkou důležité. Pro její zašifrování byl použit jednorázový klíč, který daná dvojice najde na druhém řádku ve společné tabulce jednorázových klíčů.

Oběžníkové komunikace
Oběžníková komunikace funguje na stejném principu jako vzájemná. Pouze s tím rozdílem, že nekomunikují jednotlivé dvojice stanovišť odděleně, ale celá skupina neboli oběžník najednou. Příjemcem jsou všichni v daném oběžníku. Tabulka jednorázových klíčů je tak společná a je distribuována všem stanovištím v daném oběžníku.

Formát zprávy v režimu oběžníkové komunikace
Formát zprávy je stejný, pouze na začátku bylo v rámci otevřené skupiny uvedeno, že se jedná o oběžníkovou zprávu, a to například pěticí stejných znaků, zde BBBBB:

125 DULEZITE BBBBB 02 ACKSD KDLSIE LDKFHD LDIEZC LDKEIF LKXXX **02008**

Obecná komunikace
Slouží v případě, že odesílatel potřebuje šifrovaně zaslat zprávu někomu, s kým nemá ustanoven vzájemný klíč a navíc s ním nesdílí žádnou oběžníkovou skupinu. Režim bylo doporučeno používat pouze ve velmi nutném případě, není-li k dispozici jiná alternativa.
Postupuje se následovně:

- Stroj se nastaví do libovolné pozice a zmáčknutím libovolných pěti kláves se v režimu šifrování vygeneruje náhodné jednorázové heslo.
- Stroj se nastaví do pozice dané denním klíčem a zašifruje se vygenerované jednorázové heslo.
- Poté se stroj přednastaví dle tohoto náhodného hesla. Vygenerovaná pětice slouží jako heslo pro úhlové nastavení pěti vnitřních šifrových disků.
- Zašifruje se zbytek zprávy.

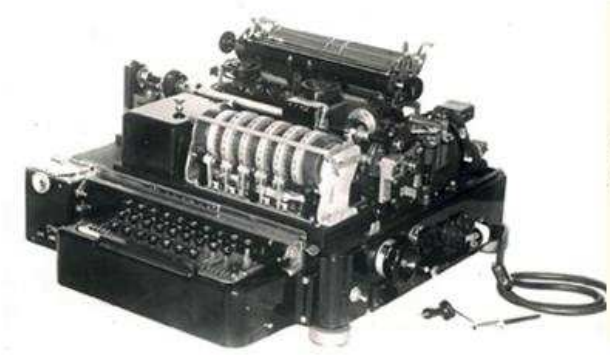
Formát zprávy v režimu obecné komunikace
Formát zprávy je podobný jako u předchozích dvou režimů. Na začátek se opět napíše adresát, důležitost, a na konec služební skupina. Před vlastní zprávou zašifrovanou vygenerovaným jednorázovým klíčem je ale navíc denním klíčem zašifrován tento jednorázový klíč.

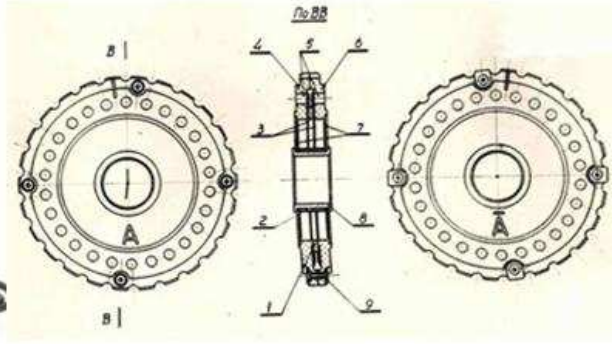
125 DULEZITE QRFSX ACKSD KDLSIE LDKFHD LDIEZC LDKEIF LKXXX **02008**

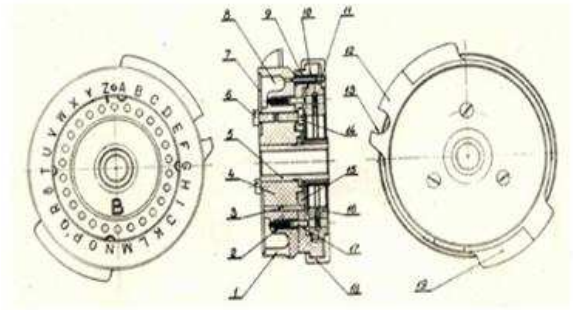
Adresát v tomto případě z formátu zprávy pozná, že se jedná o obecnou komunikaci. Nastaví stroj dle denního klíče 2. dne daného měsíce a dešifruje první pětimístnou skupinu. Tak získá jednorázový klíč pro dešifrování zbytku zprávy.

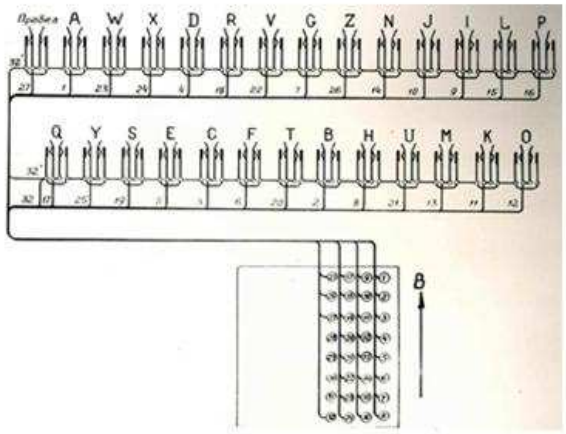
Poznámky k dešifrování
Stroj se nastavuje naprosto identicky jako při šifrování. Pouze se přepínačem druhu práce na stroji zvolí režim dešifrování.
Z formátu zprávy je na první pohled patrné, v kterém režimu a kdy byla zaslána a kdo je jejím adresátem. V závislosti na tom se pak provede dešifrování patřičného kusu zašifrované zprávy.

Obrazová dokumentace přístroje









Statistiky
V rámci testování kvality stroje jsme vyzkoušeli několik základních statistik kvality výstupního šifrového textu. Přístroj byl nastaven do náhodné polohy a zašifrován běžný český text.

Byly provedeny následující statistiky na hladině významnosti 5% v modulu Z_{26} s příslušným X^2 rozdělením:

Jednoduchá frekvenční a bigramová statistika, statistika řetězových bigramů, korelace, autokorelace, a počet znaků v pohyblivém úseku, testy monotonie.

Všechny prováděné statistiky potvrdily hypotézu, že generovaný text je na dané hladině významnosti nerozlišitelný od náhodného text. Předvádět všechny testované statistky by zabralo příliš mnoho místa, pro ilustraci proveďme test autokorelace:

Autokorelace je nástroj sloužící k hledání opakujících se vzorů v zadané posloupnosti. Hodnotu si můžeme představit jako index podobnosti různých částí vstupního textu. Pomocí ní můžeme někdy spočítat délku klíče či odhadnout slabé periody v šifrovém textu. Slabou periodu nebudeme formálně definovat. Je to taková perioda, v níž nedochází k opakování všech, ale pouze netriviálně mnoha znaků.

Nejprve zavedeme korelaci dvou posloupností.

Definice *(korelace)*: Nechť X je konečná abeceda velikosti A a $\{a_k\}$ a $\{b_k\}$ jsou dvě posloupnosti délky n nad X. Označme S, respektive R počet těch indexů, na kterých jsou hodnoty v obou posloupnostech stejné, resp. různé. Tedy $S = |\{1 \leq i \leq n; a_i = b_i\}|$ a $R = |\{1 \leq i \leq n; \{a_i i \neq b_i i\}|$. Potom korelace C mezi danými posloupnosti je číslo

$$C = \frac{A \cdot S - \frac{A}{A-1} \cdot R}{A \cdot S + \frac{A}{A-1} \cdot R} = \frac{S \cdot A\,(A-1) - R \cdot A}{S \cdot A\,(A-1) + R \cdot A}\ .$$

Poznámka 1: Pravděpodobnost shody v jednom určitém indexu je 1/A a pravděpodobnost neshody je (A-1)/A. V definici jsou jejich převrácené hodnoty.

Poznámka 2: Pro binární abecedu $X = \{0,1\}$ má vzorec tvar

$$C = \frac{S-R}{S+R} = \frac{S-R}{n}\ .$$

S touto podobou se setkáváme v moderní kryptografii nejčastěji.

Poznámka 3: Z definice korelace jsou vidět následující fakta:

- Shodují-li se posloupnosti $\{a_k\}$ a $\{b_k\}$ v n (tedy ve všech) pozicích, je korelace $C = 1$.
- Neshodují-li se posloupnosti $\{a_k\}$ a $\{b_k\}$ v žádné pozici, je korelace $C = -1$.
- Očekávaný počet shod pro dvě náhodné posloupnosti je $\frac{n}{A}$. Nastane-li právě tento počet shod, vychází $C = 0$ a říkáme, že posloupnosti jsou nekorelované.

Nyní již můžeme definovat autokorelaci. Je to korelace dané posloupnosti a posloupnosti vzniklé jejím posunem o t míst doprava. Tedy kontrolujeme shodu prvku $\{a_i\}$ s prvkem $\{a_{i+t}\}$. Takové autokorelaci budeme říkat t-autokorelace. Nás budou zajímat hodnoty t-autokorelace pro všechny možné posuny. Pokud by vyšla některá z těchto hodnot významně

vzdálená od 0, znamenalo by to, že ve vstupní posloupnosti se nachází na tomto místě slabá perioda.

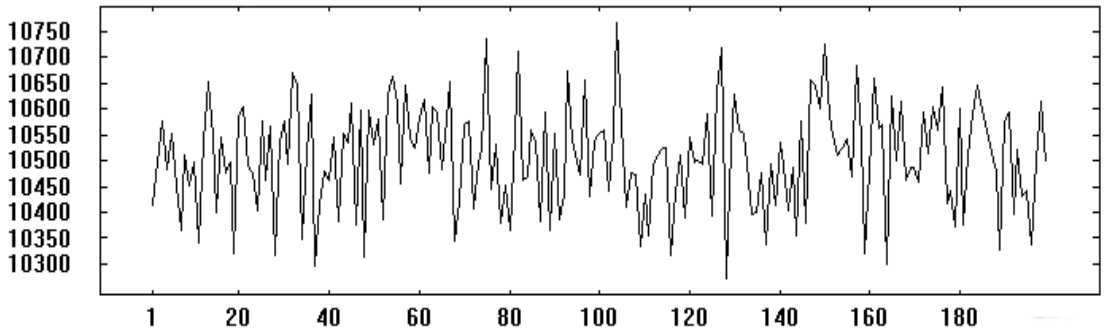
Definice *(autokorelace)*: Nechť $t \geq 1$ a $\{a_k\}$ je posloupnost délky n nad abecedou X. Konstruujme posloupnosti $\{b_k\}$ a $\{c_k\}$ délky $n-t$ takto:

- $b_i = a_i$ pro $i = 1, \ldots, n-t$
- $c_i = a_{i+t}$ pro $i = 1, \ldots, n-t$

t -autokorelace posloupnosti $\{a_k\}$ je definována jako korelace posloupností $\{b_k\}$ a $\{c_k\}$.

Nastavme nyní přístroj do testovacího nastavení dle Apendixu A a zašifrujme testovací zprávu. Zašifrovaný text označme jako posloupnost $\{a_k\}$ nad X. V našem případě $n = 273310$.
Očekávaný počet shod mezi posloupnostmi $\{b_k\}$ a $\{c_k\}$ délek $n-t$, které jsou definované v předchozí sekci, je $(n-t)/26$ a očekávaná korelace je samozřejmě nulová.

Uvádíme graf znázorňující počet shod pro prvních 200 posunů. Očekávaná hodnota se sice pro každé *t* liší, ale vzhledem k velikosti *n* je odchylka od původní hodnoty 273310/26 = 10512 zanedbatelná.



Vidíme, že odchylka od očekávané hodnoty je minimální. Nejvyšší počet shod je pro t=104, nejmenší pak pro t=128.

Kreslit graf pro všechny posuny není možné, podívejme se alespoň na extrémní hodnoty autokorelace. Testujeme pro $t = 1,2,\ldots, 10^5$. Maximální hodnota autokorelace je $0{,}0232$ a minimální $-0{,}0255$.

Závěr: Z pozorovaných hodnot můžeme konstatovat, že přístroj ŠD-2 byl navržen z pohledu korelace ideálně. Nebyla pozorována žádná odchylka od náhodného generátoru či existence slabých period.

Literatura:

[1] Brtník, V.: Bakalářská práce, katedra algebry MFF UK Praha, 2009
[2] Brtník, V.: SW simulátor ŠD-2, http://crypto-world.info/soutez2009/sd2/cti.txt
[3] Šklíba, K.: Z dějin československé kryptografie, část V., Československé šifrovací stroje z období 1955 – 1960., Šifrovací stroj ŠD – 2 (1. díl), Crypto-World 1/2008, str. 14-17
[4] Šklíba, K.: Z dějin československé kryptografie, část VI., Československé šifrovací stroje z období 1955 – 1960., Šifrovací stroj ŠD – 2 (2. díl), Crypto-World 3/2008, str. 13-22