Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 11, číslo 7-8/2009 **30. červenec 2009**

7-8/2009

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1310 registrovaných odběratelů)

Obsah : str.

Přílohy:
Simulátor šifrátoru **ŠD-2** http://crypto-world.info/soutez2009/sd2/cti.txt
(viz článek *Rekonstrukce šifrovacího stroje ŠD-2*)
Program **RSAM.EXE** (viz článek Malá soutěž v luštění RSA – řešení).
Dotazník CD Crypto-World (po vyplnění v jednom z přiložených formátů doc/rtf/txt zašlete zpět na e-zin@crypto-world.info , viz článek CD Crypto-World)

A. Do druhéhokola soutěže SHA-3 postoupilo 14 kandidátů, mezi nimi i BMW

Vlastimil Klíma, nezávislý krypotolog, (v.klima@volny.cz)

Podle oficiální zprávy z 24. 7. 2009 NIST vybral do 2. kola soutěže o nový hašovací standard **SHA-3** 14 kandidátů. Překvapením je, že nepostoupil **EDON-R**, nejrychlejší z kandidátů. Zklamáním je jistě i to, že nepostoupil **MD6**, několik let vyvíjený a snad nejvíce teoreticky rozpracovaný algoritmus, za nímž stál největší vývojový akademický tým. NIST také vybral 14 místo 15 kandidátů a udělal to dokonce o měsíc dříve, než slíbil. Algoritmy, které postoupily, uvádíme v přiložené tabulce.

K tomu je velmi vhodné si nejprve přečíst, co NIST k výběru uvedl za komentář. Vybíráme a volně překládáme:

„… Byli jsme potěšeni velkým množstvím kryptoanalýzy, učiněné v prvním kole soutěže, a poněkud ohromeni vynalézavostí některých útoků. Byli jsme také potěšeni a vděčni (i když ne překvapeni) za graciézní a přímý způsob, s nímž několik předkladatelů přijalo špatné zprávy a potvrdilo útoky nebo slabiny svých návrhů.

Do výběru kandidátů druhého kola jsme se snažili zahrnout pouze algoritmy, o nichž si myslíme, že mají šanci být zvoleny jako **SHA-3**. Byli jsme ochotni extrapolovat rychlost u těch kandidátů, kteří měli přehnanou bezpečnostní rezervu, avšak neodpouštěli jsme prolomené algoritmy. Byli jsme více ochotni akceptovat určité slabosti (v originále zneklidňující vlastnosti) hašovací funkce, pokud je návrhář připustil, než když je nepřipustil, i když měly zřejmou nápravu. Byli jsme celkově znepokojeni útoky na kompresní funkce, které předkladatelé nepřipustili.

Krátce po této zprávě zveřejníme prohlášení, v němž u každého algoritmu druhého kola popíšeme to, co se nám na návrhu líbilo i veškeré přetrvávající obavy, které máme. Vyzýváme předkladatele, aby (pokud chtějí) vylepšili své návrhy pomocí drobných změn a odstranili všechny nekonzistence a nedostatky ve specifikaci nebo zdrojovém kódu, a to do 15. 9. 2009…“

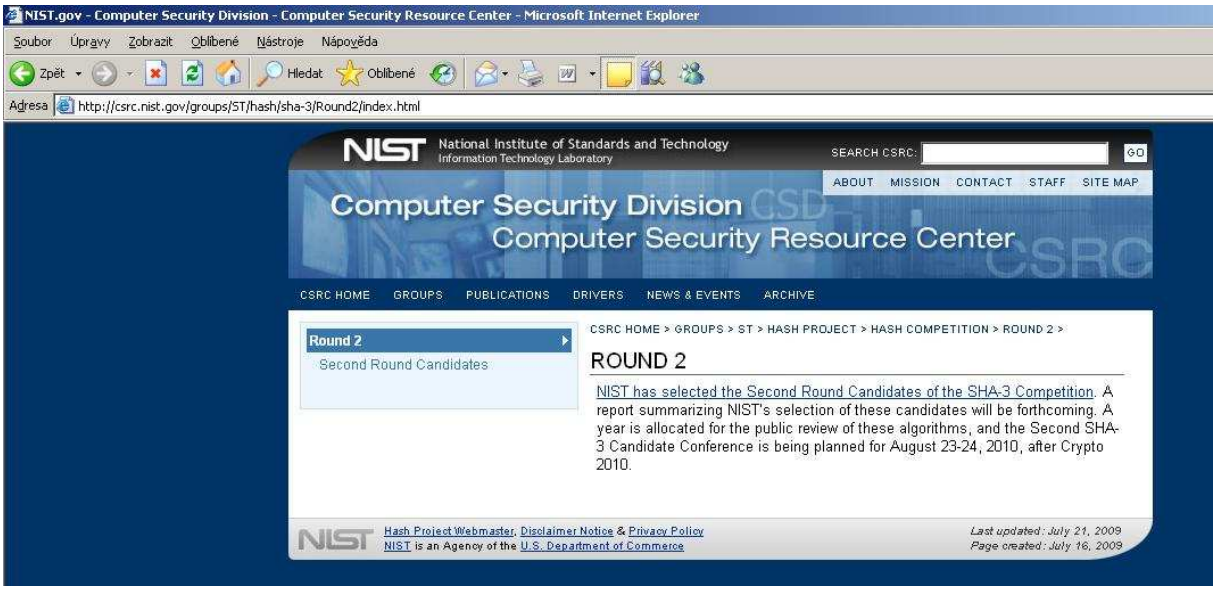
Doplňme, že *tweaks* neboli drobné změny, jsou nyní klíčovým bodem. Pomocí nich mohou předkladatelé mírně změnit své algoritmy tak, že se významně posílí nebo významně urychlí nebo obojí (☺). Nesmí přitom zásadním způsobem změnit algoritmus! Diskuse i představy NISTu na téma, co jsou drobné změny, proběhla dosti obsáhle, takže všichni tuší, co si mohou dovolit, ale každý se toho bojí. Řada algoritmů bude ubírat na bezpečnosti a zvyšovat rychlost. Například prof. Bernstein zareagoval okamžitě a u svého **CubeHash** zvýšil rychlost o více než jeden řád! Nově se do popředí v rychlosti mohou dostat algoritmy, které nepřivábily tolik pozornosti dříve a nenápadně "postávaly opodál". Drobná změna je může vyhoupnout na špici rychlosti a současní favorité se mohou ztratit v pelotonu. Všechno, co platilo dosud, už neplatí, a bude nově nastoleno až 15.9. Po tomto datu už nelze očekávat, že by se v algoritmech dělaly drobné změny, ale pouze změny "miniaturně kosmetické". Jinými slovy, kostky jsou znovu vrženy, a to, že **Blue Midnight Wish (BMW)** je momentálně nejrychlejší, neznamená do 15. 9. vůbec nic navíc.

Jisté je jen to, že vítěz musí být rychlejší a bezpečnější než SHA-2.

Algoritmus	64bit	32bit	Autorský tým, poznámka
BMW	7/3	7/12	Mezinárodní tým 6 lidí, Gligoroski, Knapskog, El-Hadedy, Amundsen, Mjølsnes (Norw. Univ.), Klima
Shabal	8	10	Francouzský tým 14 lidí (DCSSI, EADS, Fr. Telecom, Gemalto, INRIA, Cryptolog, Sagem)
BLAKE	8/9	9/12	Mezinárodní tým 4 lidí, Aumasson, Henzen, Meier, Phan (Switzerland, UK)
SIMD	11/12	12/13	Francouzský tým 3 lidí, Leurent, Bouillaguet, Fouque
Skein	7/6	21/20	Mezinárodní tým 8 lidí, Schneier, Ferguson, Lucks, Whiting, Bellare, Kohno, Callas, Walker
CubeHash	160/160 13/13	200/200 13/13	Dan Bernstein, (Univ. of Illinois),v 2. řádku rychlost uvažovaného tweaku
SHA-2	20/13	20/40	NIST, stávající standard (nesoutěží, pouze pro srovnání)
JH	16	21	Hongjun Wu, Inst. for Inf. Res., Singapore
Luffa	13/23	13/25	Mezinárodní tým 3 lidí, Canniere (Kath. Univ. Leuven), Sato, Watanabe (Hitachi)
Hamsi	25	36	Özgül Kücük (Kath. Univ. Leuven)
Grøstl	22/30	23/36	Mezinárodní tým 7 lidí, Gauravaram, Mendel, Knudsen, Matusiewicz, Rechberger, Schlaeffer, Thomsen
SHAvite-3	26/38 18/28	35/55 26/35	Izraelský tým (Dunkelman, Biham), s Intel AES instrukcemi 8 cyklů/bajt, Bernsteinova měření viz 2. ř.
Keccak	10/20	31/62	Mezinárodní tým 4 lidí (Bertoni, Daemen, Peeters, Van Assche, STM, NXP)
Echo	28/53	32/61	Mezinárodní tým 7 lidí (Billet, Gilbert, Rat, Peyrin, Robshaw, Seurin), Intel AES instr. ho urychlí
Fugue	28/56	36/72	Americký tým 3 lidí Halevi, Hall, Jutla (IBM)

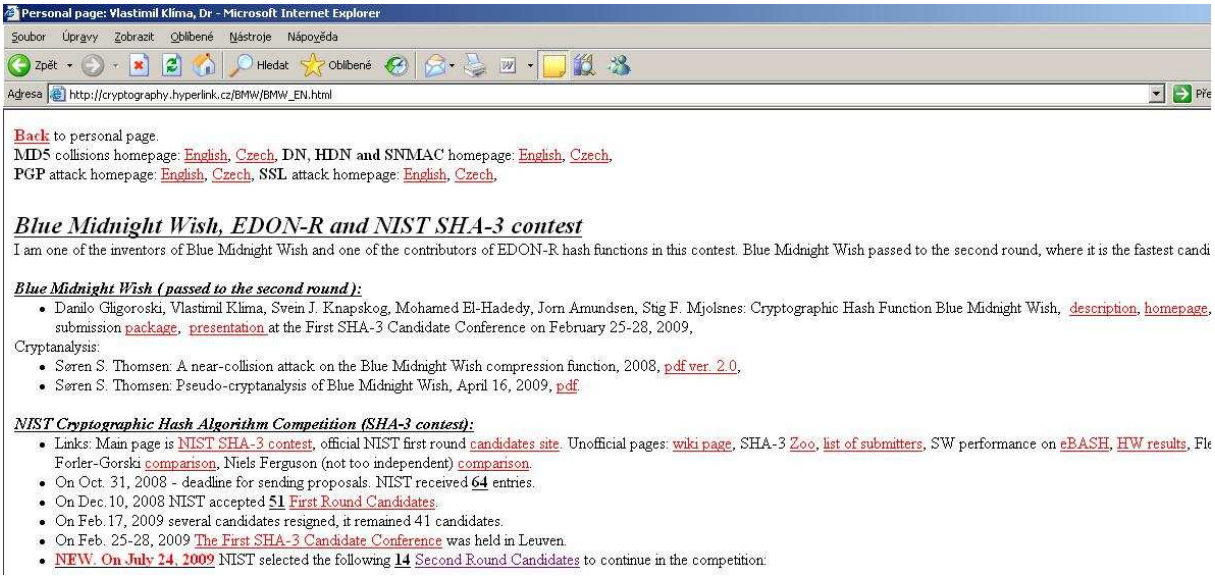
Tabulka: Rychlost kandidátů v cyklech na bajt pro 64/32bitové procesory (1./2. sloupec) a pro 256/512 bitové varianty hašovacích funkcí (v buňce tabulky)

Odkazy



[1] Informace o 2. kole:

http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/index.html



[2] Stránka autora s novinkami o soutěži a algoritmu BMW:

http://cryptography.hyperlink.cz/BMW/BMW_EN.html

[3] Klíma, V.: Blue Midnight Wish, kandidát na SHA-3 aneb poněkud privátně o tom, jak jsem k BMW přišel, Crypto-World 2/2009, str. 2-12

B. Datové schránky a co s nimi dál?

Mgr. Tomáš Sekera, YOUR SYSTEM, spol. s r.o., komerční ředitel
(tomas.sekera@gmail.com)

1. Úvod

Datové schránky jsou na světě, jsou po počátečních porodních bolestech funkční a pro řadu komerčních organizací a hlavně orgánů veřejné moci nastala zásadní otázka – jak dokumenty přijaté z datové schránky dále zpracovávat. Prosté přijetí je přitom relativně nejsnazší záležitostí. Adresáti se ale musí vyrovnat zejména s tím, jak datové zprávy včetně obsahu důvěryhodným způsobem uchovávat po celou dobu jejich životního cyklu a přitom k nim přidávat dokumenty další anebo je kombinovat s listinnou podobou souvisejících dokumentů. Současně budou prostřednictvím datových schránek odpovídat nebo sami podání vytvářet. Zároveň je třeba domyslet i konečnou fázi, kterou je archivace vybraných dokumentů.

Stát uložil zákonem povinnost, v některých případech možnost, datové schránky pro nyní vybranou komunikaci využívat. Přitom je předpokládáno zásadní rozšíření této komunikace a to ve smyslu zasílání faktur, následně i dodávání jiných sdělení. S datovými schránkami se proto musíme naučit žít…

2. Jak na to

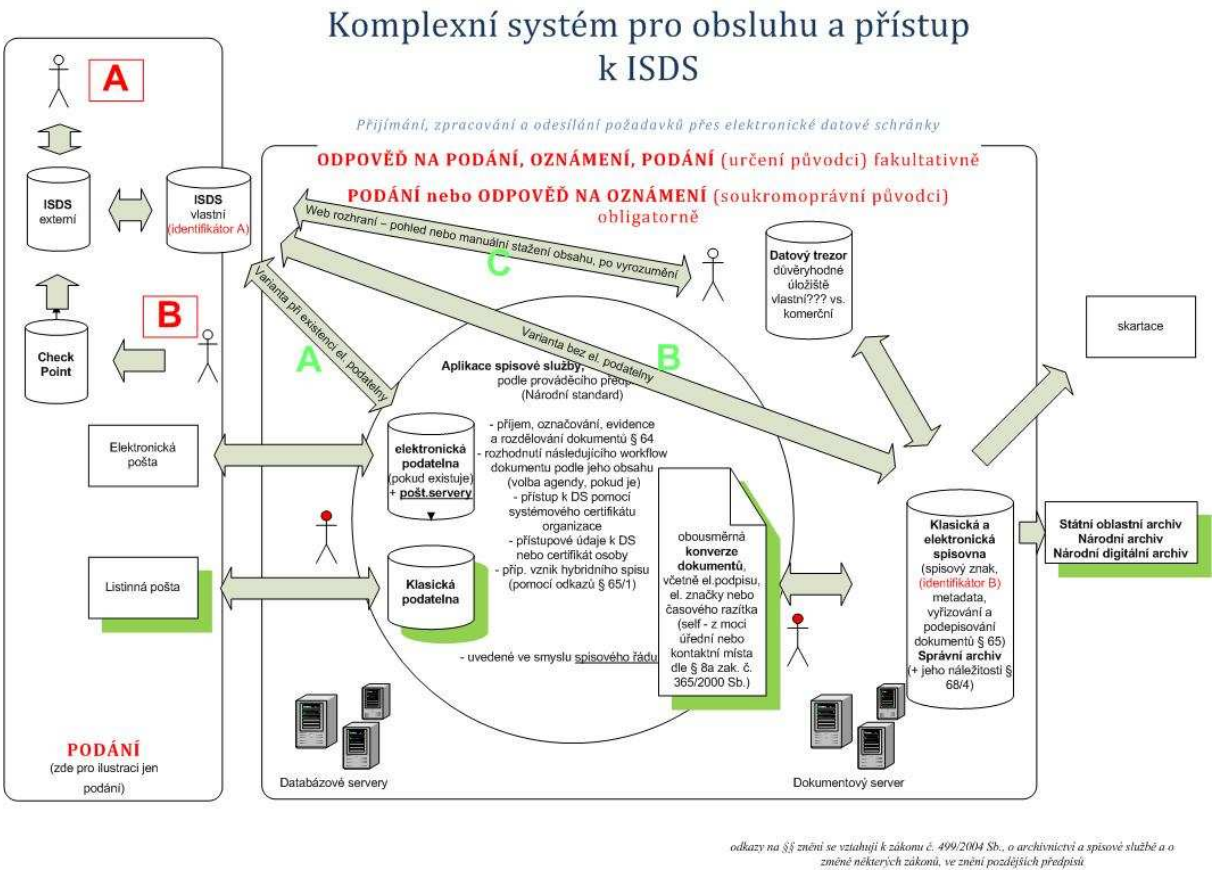
Smyslem tohoto článku není, ani nelze, popsat jednoduché řešení, ale poukázat na nutnost koncepčního myšlení při zavádění komunikace prostřednictvím datových schránek a nezbytnost spolupráce dotčených interních celků organizace při takové procesní „revoluci“.

Úvodem je třeba říci, že univerzální všeobjímající řešení neexistuje. Uvedené z důvodu, že účastníci celého procesu na straně adresáta, který bývá i odesilatelem zpráv, mají odlišné právní povinnosti a využívají nebo nevyužívají související agendy. K tomu přistupuje fakt, že většina větších organizací nějakým způsobem již části požadovaných funkcionalit spisové služby má nastaveny, při dosavadním vynaložení nemalých finančních prostředků.

Dovolil jsem si níže uvést schematický nákres hlavních požadovaných funkcionalit systému pro zpracování zpráv z datových schránek. Schéma zahrnuje i nástin souvisejících povinností. Jak ale již bylo napsáno, nikoliv všechny zúčastěné subjekty musí splnit veškeré povinnosti.

V praxi se přitom ukazuje, že zavedení datových schránek je vlastně spouštěcím mechanismem k revizi současné spisové služby, souvisejících workflow dokumentů, případně k přenastavení Document Management System (DMS), Contract Management, vstupů a výstupů do účetních systémů, scanovacích mechanismů pro obousměrnou konverzi dokumentů, poštovních mail serverů, podatelny, vyhodnotit a nastavit používání el. podpisu, značky a časového razítka, nastavit parametry datových skladů, akceptovat hierarchii organizačních jednotek a odpovědností, zavést provázanost různých identifikátorů – pokud tyto celky vůbec existují. Jedná se o kvalitativní i kvantitativní update celé řady interních procesů. Nelze opominout ani zaškolení obsluhy a uživatelů. Současně je evidentním, že pokud má celý systém řízeného toku elektronických dokumentů v organizaci řádně fungovat, je nutno zajistit provázanost a odpovídající úroveň všech dotčených systémů a procesů, ačkoliv zákon explicitně takovou povinnost všem subjektům neukládá.

Z povahy věci plyne, že problém lze a je žádoucí řešit jen koncepčně, za účasti všech zástupců interních organizačních jednotek (např. IT/HW, SW, infrastruktura, architektura, dále archivní a právní odbor, vlastní podatelna, spisovna anebo jejich síť, odbor bezpečnosti) a dodavatelů jednotlivých částí komunikačního systému. Zavedení komunikace prostřednictvím datových schránek, bez návaznosti na další procesy již pro organizaci střední velikosti může být riskantní zejména z pohledu nereagování na podněty v zákonných lhůtách, neunesení budoucího důkazního břemene (např. integrita elektronického dokumentu v čase, prokázání místa a času doručení), neschopnosti vybrané dokumenty v elektronické podobě řádně archivovat. Přeloženo – hrozí značné a zásadní škody



Uživatelům datových schránek lze jen doporučit, aby jednotlivé části celého komunikačního systému řešili formou projektu. Na počátku je nutné provést analýzu současného stavu a porovnat s výstupy zákonných a obchodních potřeb. V neposlední řadě klasifikovat dokumenty, u kterých předpokládáme, že budou vstupovat a vystupovat do systému datových schránek, resp. do systému elektronické komunikace celé organizace. Stanovit rozsah a etapy projektu. Požadavky na finanční a lidské zdroje, dodavatele, případně outsourcing. Řešením tedy není „pouhé“ zajištění přístupu ke zprávám, či nasazení elektronické spisové služby, včetně různých modulů, ale koncepční záměr řídit elektronickou komunikaci v organizaci. Do úvahy přichází pro snížení rizika nezachování zprávy a jejích příloh, resp. spisu v odpovídající podobě, možnost do doby realizace celého projektu využívat k uložení důvěryhodné úložiště vybraných dokumentů. Takové úložiště lze jistě postavit vlastní, ale pro přechodné období nebo pro menší organizace se jeví výhodnějším použít některé z nabízených komerčních řešení, jež nyní nabízejí Česká pošta a TO2, s určitou mírou garance.

3. Jsou datové schránky i ekonomickou výhodou – pro uživatele?

Zavedení datových schránek přinese nepochybně zrychlení a zjednodušení komunikace uvnitř státní správy a se státní správou, resp. orgány veřejné moci. Přinese snížení nákladů i v souvislosti s odpadnutím klasické poštovní přepravy dokumentů.
Na druhé straně přináší orgánům veřejné moci, tedy státu samotnému, ale i komerčním subjektům plnění celé řady povinností a s tím souvisejících investičních a provozních nákladů při nastavení, rozšíření a provozu souvisejících systémů.
Zda datové schránky budou i ekonomickým přínosem a pro koho ukáže až čas, kdy bude možné porovnat úspory, efektivitu a skutečně vynaložené náklady.
K samostatnému zamyšlení je využívání datových schránek pro rozesílání a příjem faktur. Jelikož odpovídající a funkční systémy pro fakturaci (např. EDI) pro velké uživatele již existují, uvidíme, kdo a jakým způsobem bude vůbec datové schránky za tímto účelem používat.

4. Realizace komunikace prostřednictvím datových schránek v čase

Na straně státu jako provozovatele datových schránek je jeho povinnost relativně již splněna. Dovolím si kacířskou otázku. Budou všichni určení a soukromoprávní původci zcela a skutečně připraveni po plynutí zákonného přechodného období k takové komunikaci? Osobně bych se přimlouval k prodloužení přechodného období, minimálně do konce tohoto kalendářního roku a to právě z důvodu nutnosti faktické reorganizace řady procesů na straně uživatelů.

5. Závěr

Datové schránky jsou počinem pro rychlejší a efektivnější vybranou komunikaci. Nepřímo nutí uživatele zlepšit řízení toku dokumentů v organizaci jako celku. Nejedná se o zřízení státního freemailu, dopady této formy doručování jsou z pohledu práva opravdu revoluční. Nezbývá, než popřát uživatelům úspěch a pokud možno minimalizované náklady při nejen příjmu a odesílání zpráv, ale v celém řízení komunikace v organizaci.

C. Rekonstrukce šifrovacího stroje ŠD-2

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

V roce 2008 byl v Crypto-Worldu (CW 1/2008, CW 3/2008) představen rotorový šifrovací stroj ŠD-2. Věnovali jsme se jeho původu a stručnému popisu funkčnosti. V následujícím článku, který si stručně zopakujeme známé skutečnosti a přidáme nové: detailní popis šifrovací jednotky, obrazovou dokumentaci a soubor statistických testů. Jedná se o část výsledků z mé bakalářské práce [1] (vedoucí práce P.Vondruška), kterou jsem v roce 2009 na katedře algebry MFF UK Praha úspěšně obhájil. Součástí práce je i SW simulátor šifrátoru ŠD-2 [2].

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.

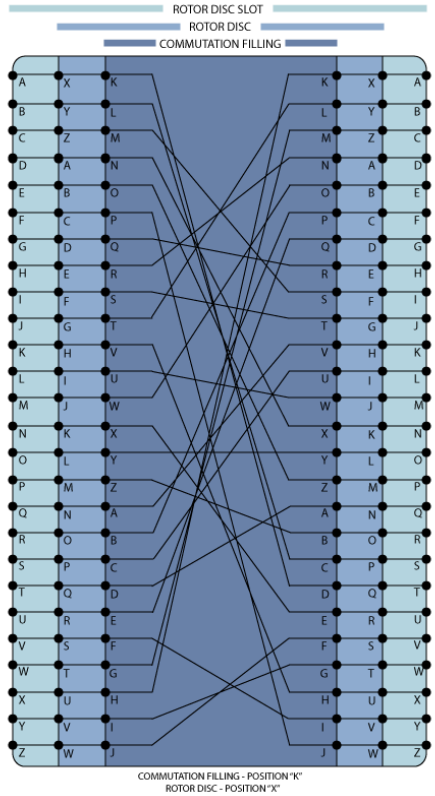
Pravý pevný disk

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.



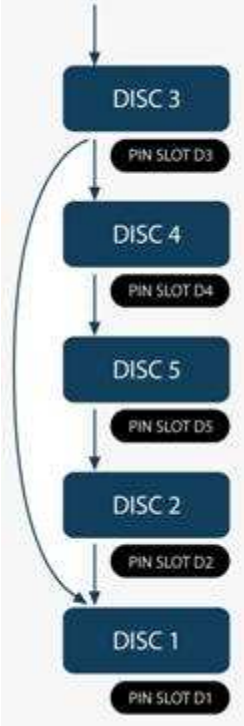
Černými čarami je vyznačeno 26 elektrických vodičů tvořících 26 elektrických obvodů. Tmavě modrou barvou je naznačena komutační vložka, světlejší je pak vlastní disk. Ten se v každém kroku otáčí a otáčí také komutační vložkou, která je v něm vložena. Jednotlivá písmena na obvodu komutační vložky i pevného 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.

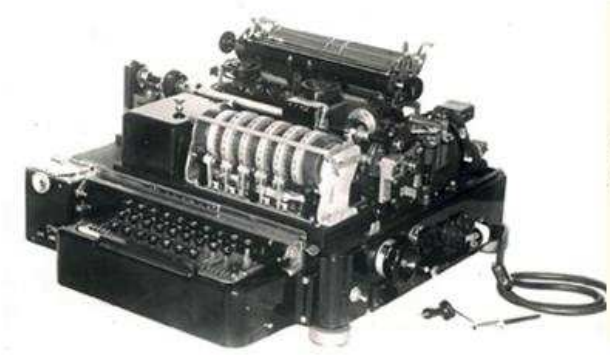
Formát zprávy v režimu obecné komunikace
Formát zprávy je podobný jako u předchozích dvou režimů. Na začátek se opět napíše adresát, důležitost, a na konec služební skupina. Před vlastní zprávou zašifrovanou vygenerovaným jednorázovým klíčem je ale navíc denním klíčem zašifrován tento jednorázový klíč.

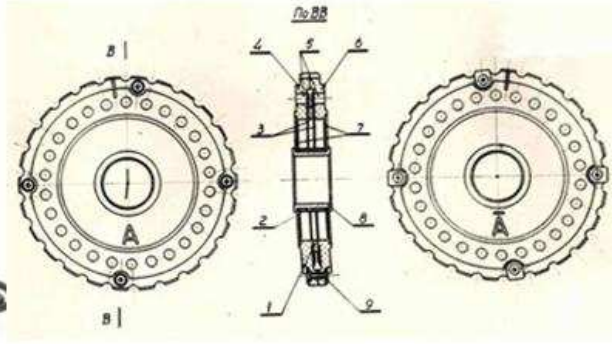
125 DULEZITE QRFSX ACKSD KDLSIE LDKFHD LDIEZC LDKEIF LKXXX **02008**

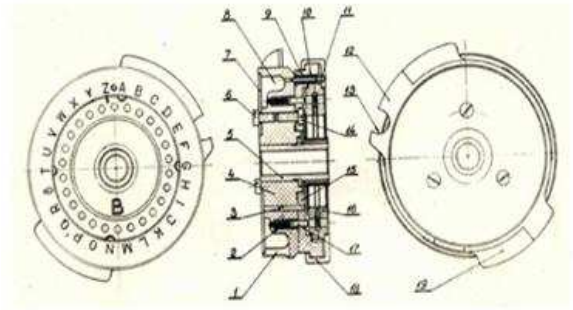
Adresát v tomto případě z formátu zprávy pozná, že se jedná o obecnou komunikaci. Nastaví stroj dle denního klíče 2. dne daného měsíce a dešifruje první pětimístnou skupinu. Tak získá jednorázový klíč pro dešifrování zbytku zprávy.

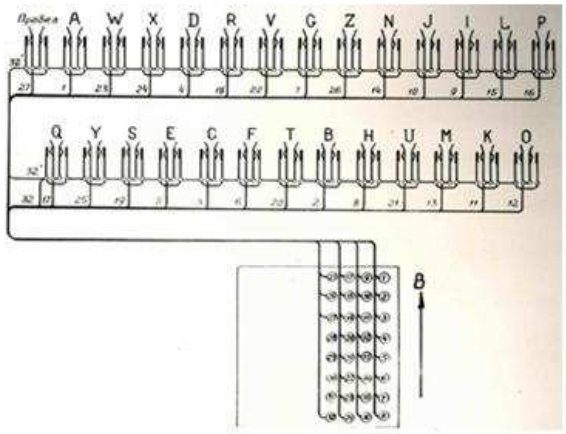
Poznámky k dešifrování
Stroj se nastavuje naprosto identicky jako při šifrování. Pouze se přepínačem druhu práce na stroji zvolí režim dešifrování.
Z formátu zprávy je na první pohled patrné, v kterém režimu a kdy byla zaslána a kdo je jejím adresátem. V závislosti na tom se pak provede dešifrování patřičného 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 $S = |\{1 \le i \le n; a_i = b_i\}|$ a $R = |\{1 \le i \le n; \{a_1 i \neq b_1 i\}|$. Potom korelace C mezi danými posloupnosti je číslo

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

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

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

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.

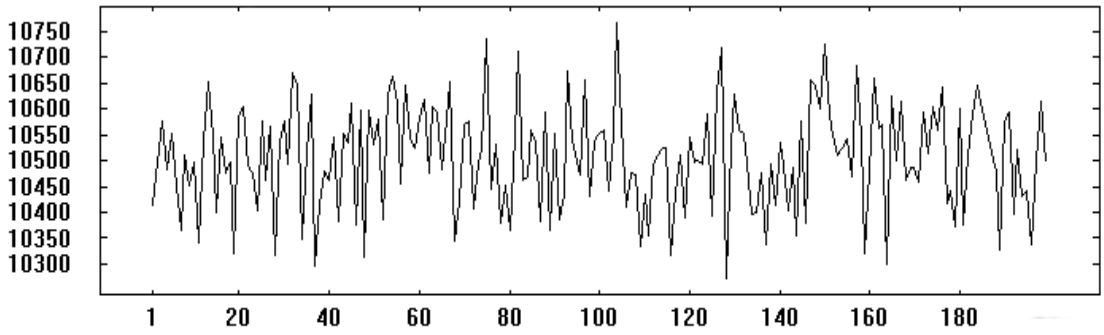
Definice *(autokorelace)*: Nechť $t \geq 1$ a $\{a_k\}$ je posloupnost délky n nad abecedou X. Konstruujme posloupnosti $\{b_k\}$ a $\{c_k\}$ délky $n-t$ takto:

- $b_i = a_i$ 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

D. Malá soutěž v luštění RSA - řešení

Pavel Vondruška (pavel.vondruska@crypto-world.info)

ÚLOHA

V minulém čísle e-zinu Crypto-World byla zveřejněna následující úloha:

Soutěžící má za úkol rozluštit šifrový text
14 39 07 57 18 34 10 47 17 92 06 31 28 65 32 92 11 41 26 31
26 29 20 80 25 06 00 77 03 60 09 00 03 60 11 44 31 00 05 41
07 92 06 16 04 70 10 75 03 60 18 79 00 46 26 73 23 49 25 18 13 90,

kde k zašifrování otevřeného textu byl použit algoritmus RSA, veřejný klíč (N,e)=(3337, 79) a formátování CW#1.0 (detaily k úloze viz e-zin Crypto-World 6/2009, Malá soutěž v luštění RSA str.19-20, resp. závěrečný odstavec tohoto článku **Doplňující informace k soutěžní úloze**).

POŘADÍ

E-zin s úlohou byl rozeslán 15.června 2009 ve 22:56. Již za půl hodiny po rozeslání kódů k jeho stažení jsem obdržel prvé správné řešení! Další řešení pak postupně následovala. Správné řešení zaslalo celkem deset čtenářů. Všem úspěšným luštitelům blahopřeji.

Přehled úspěšných řešitelů:
1) Michal Kesely, 15.červen 2009, 23:32
2) Petr Veselý, 15.červen 2009, 23:48
3) Jan Klimeš, 16.červen 2009, 7:31
4) Zdeněk Orság, 16.červen 2009, 8:52
5) Kocfelda (koc), 16.červen 2009, 9:20
6) Pavel Noga, 16.červen 2009, 18:01
7) Jan Prichystal, 17.červen 2009, 21:40
8) František Půbal (OK1DF), 17.červen 2009, 22:11
9) Lubor Otta, 19.červen 2009, 16:32
10) Pavel Hanák (Winetou), 19.červen 2009, 21:53

ŘEŠENÍ

Řešení spočívá ve výpočtu soukromého klíče z veřejného klíče. Toto je možné provést poměrně snadno, neboť prvočísla použitá v soutěžním příkladě jsou příliš malá. Připomeňme, že pro reálný algoritmus RSA se v praxi používají prvočísla délky 155 dekadických čísel. Při použití takovýchto prvočísel má získaný modul délku 1024 bitů…
Po zisku soukromého klíče se následně provede dešifrace soutěžní úlohy. Při dešifraci je potřeba zachovávat pravidla formátování CW#1.0. Tím je úloha vyřešena.

Veřejný klíč: (N,e)=(3337, 79)

1) Faktorizace (rozklad na prvočísla) N=3337 je triviální a brzy se nám podaří najít příslušná prvočísla p=47 a q=71 (47*71=3337).
2) Spočteme $\Phi(N) = (p-1)*(q-1)$, $\Phi(N) = 46*70=3220$.
3) Z rovnice $e*d \equiv 1 \bmod \Phi(N)$ vypočteme soukromý exponent d a tím získáme soukromý klíč (d,N).

Po dosazení známých hodnot získáme rovnici: $79*d \equiv 1 \bmod \Phi(3220)$

$d = 1019$ (k výpočtu použijeme Eukleidův algoritmus)

Výpočet inverze 79 v Z 3220 je poněkud pracnější. Někteří luštitelé k tomu použili program Mathematica, jiní si napsali vlastní prográmek. Výsledek však lze (vzhledem k malým číslům) poměrně brzy získat i „zkusmo“.

Hledaný soukromý klíč je (1019, 3337)

4) Nyní můžeme přistoupit k řešení úlohy.

14 39 07 57 18 34 10 47 17 92 06 31 28 65 32 92 11 41 26 31
26 29 20 80 25 06 00 77 03 60 09 00 03 60 11 44 31 00 05 41
07 92 06 16 04 70 10 75 03 60 18 79 00 46 26 73 23 49 25 18 13 90 .

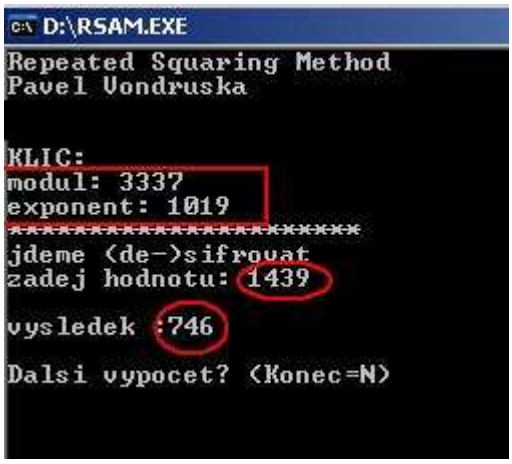
Vzhledem ke 4-cifernému modulu 3337 a pravidlům formátování přepíšeme šifrový text na tvar (C_1 C_2 C_3 … C_i)

1439 0757 1834 1047 1792 0631 2865 3292 1141 2631
2629 2080 2506 0077 0360 0900 0360 1144 3100 0541
0792 0616 0470 1075 0360 1879 0046 2673 2349 2518 1390 ,

Nyní již můžeme přistoupit k dešifrování

(viz $m_1 \equiv C_1^d \bmod N$, $m_2 \equiv C_2^d \bmod N$, $m_3 \equiv C3^d \bmod N$ .... $m_i \equiv C_i^d \bmod N$)

Vzhledem k velkým číslům je potřeba k výpočtu použít buď program Mathematica nebo si napsat vlastní program. Pro samotný výpočet se používá metoda „Repeated Squaring Method“. V příloze k e-zinu přikládám můj jednoduchý prográmek RSAM.EXE, výstup z programu viz obrázek).



Postupně vypočteme:

$m_1 \equiv C_1^d \bmod N$, $m_1 \equiv 1439^{1019} \bmod 3337 = 746$,

$m_2 \equiv C_2^d \bmod N$, $m_2 \equiv 757^{1019} \bmod 3337 = 575$, atd.

1439	757	1834	1047	1792	631	2865	3292	1141	2631	
746	575	706	885	756	590	906	974	838	469	
2629	2080	2506	77	360	900	360	1144	3100	541	
868	982	698	373	767	385	767	972	859	65	
792	616	470	1075	360	1879	46	2673	2349	2518	1390
837	669	846	983	767	986	798	372	657	773	820

Získané výsledky doplníme podle pravidel pro formátování CW#1.0 do skupin délky 3 (v příkladě je potřeba provést pouze u 65 / 065). Je zajímavé, že toto pravidlo formátování činilo některým řešitelům potíže, a tak těsně před branou vítězství se jim nepodařilo získat správný výsledek, protože konec otevřeného textu jim bez uvedené úpravy nedával smysl.

```
746 575 706 885 756 590 906 974 838 469 868 982 698 373 767 385
767 972 859 065 837 669 846 983 767 986 798 372 657 773 820
```

Následně rozdělíme text do dvoumístných skupin, abychom mohli provést dekódování podle převodové tabulky uvedené v pokynech pro formátování zprávy:

```
74 65 75 70 68 85 75 65 90 90 69 74 83 84 69 86 89 82 69 83 73 76 73 85 76
79 72 85 90 65 83 76 69 84 69 83 76 79 86 79 83 72 65 77 73 82 0
```

Po dekódování podle převodové tabulky již získáme otevřený text soutěžní úlohy:

```
74 65 75 70 68 85 75 65 90 90 69 74 83 84 69 86 89 82 69 83 73 76 73 85 76
J  A  K  F  D  U  K  A  Z  Z  E  J  S  T  E  V  Y  R  E  S  I  L  I  U  L

79 72 85 90 65 83 76 69 84 69 83 76 79 86 79 83 72 65 77 73 82
O  H  U  Z  A  S  L  E  T  E  S  L  O  V  O  S  H  A  M  I  R
```

Soutěžícím se omlouvám za chybu, která se mi vloudila do úlohy při přípravě (JAKF /JAKO). Úspěšní řešitelé se tímto neúmyslným problémem nenechali zmást a úlohu dokončili správně a zaslali jako důkaz vyřešení úlohy požadované slovo **SHAMIR**, tedy jméno jednoho ze tří kryptologů, kteří systém RSA vymysleli.

Profesor Adi Shamir.

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

DOPLŇUJÍCÍ INFORMACE K SOUTĚŽNÍ ÚLOZE

1. Použitý šifrovací algoritmus

Jedná se o klasický šifrovací algoritmus založený na RSA, kde však otevřený text není formátován podle PKCS #1 (verze 1.5,2.0,2.1), ale podle námi zadaných pravidel, která označíme jako CW #1.0.

2. Asymetrický algoritmus RSA

Zvolíme prvočísla p a q a vypočteme

$N = p*q$

$\Phi(N) = (p-1)* (q-1)$

Dále náhodně vybereme číslo e, kde

$1 < e < \Phi(N)$, takové, že e a $\Phi(N)$ jsou nesoudělná.

Vypočteme číslo d takové, že

$1 < d < \Phi(N)$ a

$e*d \equiv 1 \mod \Phi(N)$

Dvojici (N, d) nazveme soukromý klíč a (N, e) veřejný klíč.

3. Formátování zprávy (CW#1.0)

Zprávu M překódujeme nejprve do číselného tvaru. K tomu použijeme některou vhodnou převodovou tabulku, např. tuto:

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

Zprávu M pak zformátujeme do posloupnosti čísel pevné délky (délka bude rovna délce modulu N). K tomu použijeme vlastní formátování, která pracovně nazveme CW#1.0:

Formátování CW#1.0 :

1) Má-li modul délku k, budeme zprávu převedenou podle tabulky dělit na skupiny délky k-1.
2) Všechny skupiny musí mít délku k-1, nemá-li proto poslední skupina tuto délku, doplníme ji zprava příslušným počtem nul.
3) Všechny získané skupiny nyní doplníme zleva jednou nulou. Délka každé skupiny je po těchto úpravách rovna k.
4) Výsledek po šifrování má délku rovnou maximálně k. Pokud je délka menší, doplníme výsledek zleva nulami do délky k.

Výsledek získaný po formátování zprávy M označme $m_1\ m_2\ m_3\ \ldots$

4. Zašifrování zprávy M

Zašifrováním zprávy M pomocí veřejného klíče (N,e) rozumíme řetězec

$P = C_1\ C_2\ C_3\ \ldots\ .$, kde

$C_1 \equiv m_1^e \mod N$, $C_2 \equiv m_2^e \mod N$, $C_3 \equiv m_3^e \mod N$ ..... $C_i \equiv m_i^e \mod N$

5. Dešifrování zprávy P

Dešifrování zprávy P se provede tak, že použijeme soukromý exponent d a tím získáme původní zprávu M

$m_1 \equiv C_1^d \mod N$, $m_2 \equiv C_2^d \mod N$, $m_3 \equiv C_3^d \mod N$ .... $m_i \equiv C_i^d \mod N$

E. CD Crypto-World

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Nově registrovaní čtenáři se mne často ptají, zda je možné získat všechna dosud vyšlá čísla e-zinu Crypto-World jiným způsobem než postupným a pracným stahováním z domovské stránky http://crypto-world.info/. Z tohoto důvodu jsem se rozhodl **nabídnout k jedenáctému výročí založení e-zinu speciální CD (prvé číslo vyšlo 7. září 1999),** které by obsahovalo všechna dosud vyšlá čísla včetně příloh a dále vybraný SW, který byl speciálně vytvořen v rámci soutěží 2000-2009 a některé další související materiály, které jsou k dispozici na webu (např. knihu Elektronický podpis, moje starší články apod.).

Abych si ověřil **reálný zájem** o toto CD a zda vůbec má smysl tuto službu zavést, rozhodl jsem se vás požádat o vyplnění dotazníku (uveden v příloze) a jeho zaslání ke zpracování a vyhodnocení na adresu ezin@crypto-world.info .

Pokud bude o CD zájem, pak jej připravím a na základě závazné objednávky, která bude dostupná na webu Crypto-World a uvedena jako příloha v e-zinu Crypto-World 9/2009, jej budu rozesílat.

Za všechny vyplněné dotazníky a zaslané reakce předem děkuji.

Pavel Vondruška

Dotazník

(prosím odpovídejte nezkresleně, vyplnění vás k ničemu nezavazuje a je dobrovolné, zveřejněna bude pouze celková statistika, dotazník ve formátech txt/doc/rtf/ najdete v příloze k tomuto e-zinu)

1) Myslím si, že je to dobrá služba **ANO / NE**
2) Měl bych zájem si CD pořídit **ANO / NE**
3) Cena 120,- Kč (včetně balného a poštovného) mi připadá **nízká/odpovídající/vysoká**
4) Měl bych zájem, aby na CD byla databáze všech příspěvků zveřejňovaných na webu v sekci Crypto-News a Security-News (k 31.7 již více jak 10 200 příspěvků) **ANO / NE**
5) Byl bych ochoten za CD rozšířené o databázi příspěvků zaplatit 180,- Kč (včetně balného a poštovného) **ANO / NE**
6) Platba předem převodem na účet CW je pro mne akceptovatelné řešení platby **ANO / NE**
7) Budu potřebovat předem zaslat PROFORMA FAKTURU **ANO / NE**
8) S CD budu požadovat dodání **faktury/příjmového dokladu/je mi to jedno**
9) Můj komentář:

F. O čem jsme psali v létě 2000 - 2007

Crypto-World 78/2000

Příloha : 10000.txt , soubor obsahuje prvních 10 000 prvočísel (další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

Crypto-World 78/2001

Příloha : priloha78.zip (dopis pana Sůvy - detailní informace k horké sazbě, viz. článek Záhadná páska z Prahy, Crypto-World 6/2001)

Crypto-World 78/2002

Crypto-World 78/2003

Crypto-World 78/2004

Crypto-World 78/2005

Crypto-World 78/2006

Crypto-World 78/2007

Crypto-World 78/2008

G. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/