



BIS

Bezpečnost informačních systémů

Petr Hanáček

Faculty of Information Technology

Technical University of Brno

Božetěchova 2

612 66 Brno

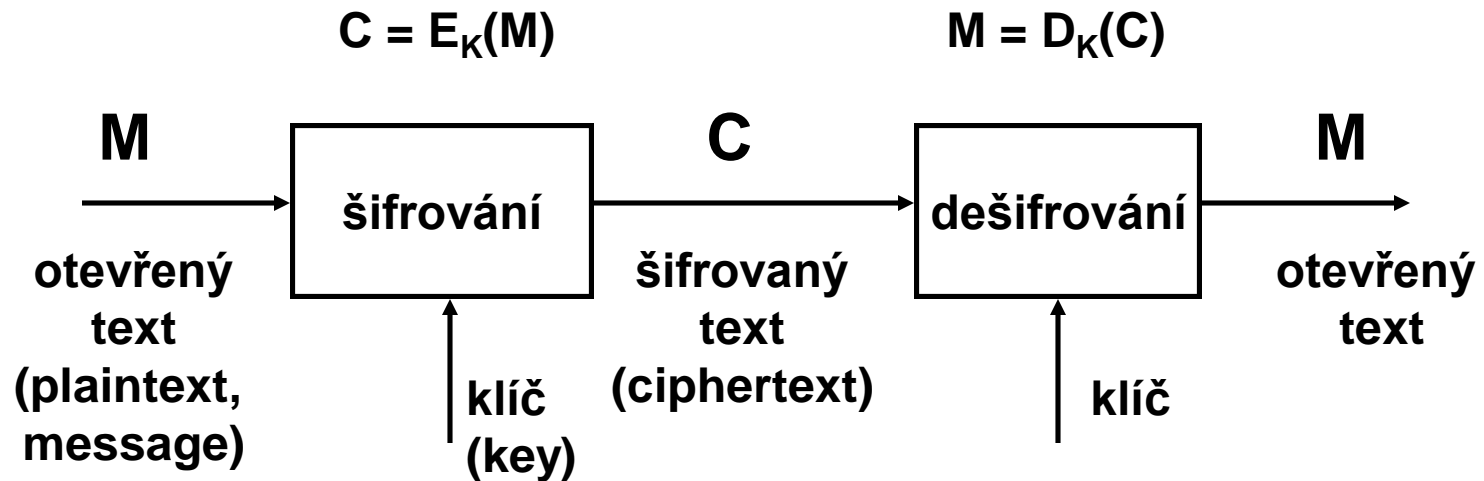
tel. 5 4114 1216

e-mail: hanacek@fit.vutbr.cz

Kryptografie

- Účel kryptografie
- Klasická kryptografie x Moderní kryptografie
 - Historie
 - Základní rozdíly

Kryptografie



- **podle klíčů**

- symetrické **X** asymetrické
- tajný klíč **X** veřejný klíč, soukromý klíč

Pojmy

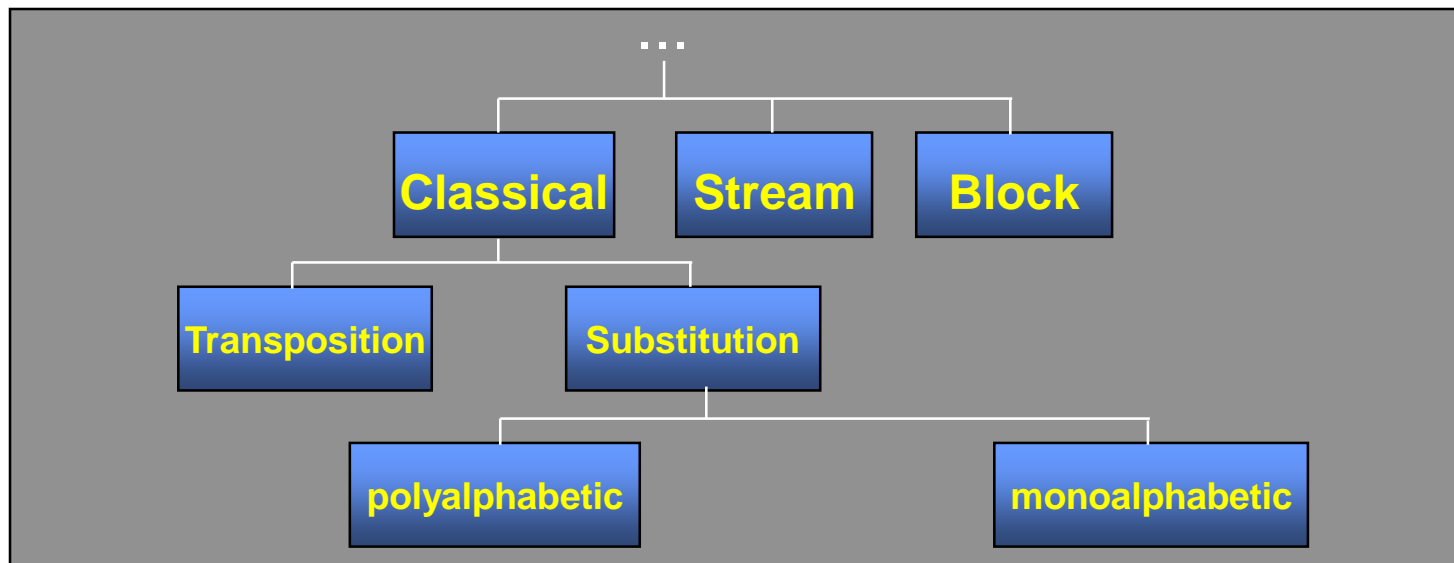
- **Kryptografie - cryptography**
 - Transformace otevřeného textu na šifrovaný text a (obvykle) naopak
- **Kryptoanalýza - cryptanalysis (codebreaking)**
 - Transformace šifrovaného textu na otevřený bez znalosti klíče
- **Kryptologie - cryptology**
 - Kryptografie a kryptoanalýza
- **Šifra, šifrovací algoritmus - cipher**
 - Algoritmus na transformaci otevřeného textu na šifrovaný text a (obvykle) naopak
- **Otevřený text**
 - Srozumitelný text, zpráva, plaintext, message
- **Šifrovaný text**
 - Kryptogram, ciphertext, cryptogram
- **Šifrování - encryption**
- **Dešifrování - decryption**

Útoky

- **Ciphertext only attack**
 - Útočník zná pouze šifrovaný text, snaží se zjistit klíč nebo otevřený text
- **Known plaintext attack**
 - Útočník zná šifrovaný text a odpovídající otevřený text, snaží se zjistit klíč
- **Chosen plaintext attack**
 - Útočník zná šifrovaný text a odpovídající otevřený text, který si mohl zvolit, snaží se zjistit klíč

Typy klasických šifer

- **Steganografické postupy**
 - ukryjí přenášený text uvnitř jiného textu
- **Substituční šifry**
 - nahrazují jednotlivé znaky/symbols textu jinými znaky
- **Transpoziční šifry**
 - mění pořadí znaků v textu (typicky pomocí nějakého geometrického obrazce, např. matice)



Steganografie

- **Stega = hidden**
- **Graph = writing**
- **Steganografie je způsob jak ukrýt informaci uvnitř něčeho jiného**
- **Příklady:**
 - **Ukrytí informace uvnitř textového souboru**
 - **Vodoznak (watermark) uvnitř obrazu**

Steganografie

Dear George, 3rd March
Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final dispatch to the Syndicate by Friday 20th or at the very least, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

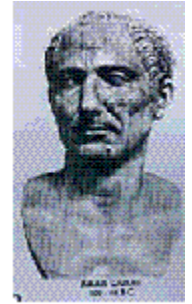
- **Například první písmeno každého slova, nejméně významný bit každého pixelu**
- **Princip „Security through obscurity“**
- **Nepoužitelná jakmile se prozradí metoda**

Steganografie

Dear George, 3rd March
Greetings to all at Oxford. Many thanks for your
letter and for the Summer examination package.
All Entry Forms and Fees Forms should be ready
for final dispatch to the Syndicate by Friday
20th or at the very least, I'm told, by the 21st.
Admin has improved here, though there's room
for improvement still; just give us all two or three
more years and we'll really show you! Please
don't let these wretched 16+ proposals destroy
your basic O and A pattern. Certainly this
sort of change, if implemented immediately,
would bring chaos.

Substituční šifry

Caesarova šifra



- První známé algoritmické šifrování
- Julius Caesar šifroval své zprávy tak, že nahradil každé písmeno třetím následujícím písmenem v abecedě
- “caesar” se zašifruje jako “FDHVDU”
- Slabiny
 - každý, kdo zná algoritmus, může zprávu dešifrovat
- Možné vylepšení
 - odesílatel a příjemce mají domluven klíč (číslo od 1 do 25), který znamená o kolik písmen se posouvá
 - šifra je stále slabá - stavový prostor klíčů je příliš malý

| | |
|-------|-------|
| a → D | w → Z |
| b → E | x → A |
| c → F | y → B |
| d → G | z → C |

Caesarova šifra - útoky

- Útok silou – pouhých 26 možností
- Frekvenční analýza

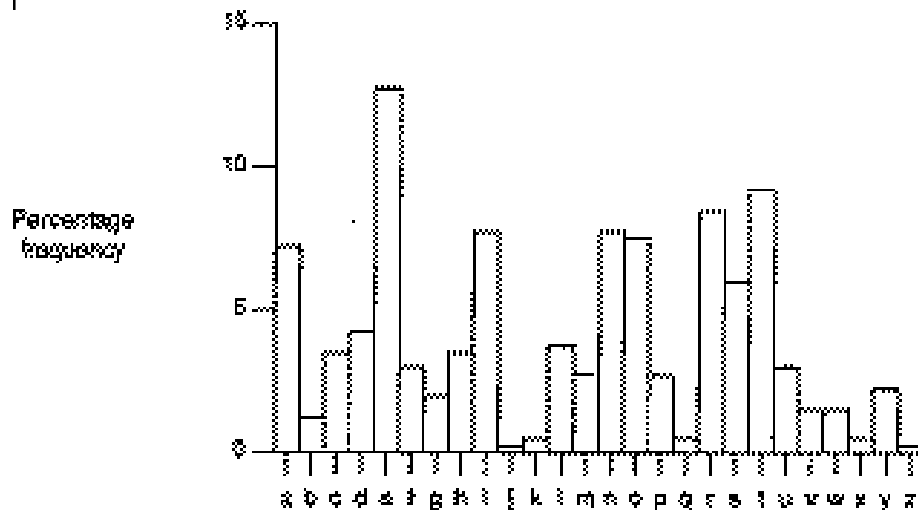


Figure 3.1 English character frequencies

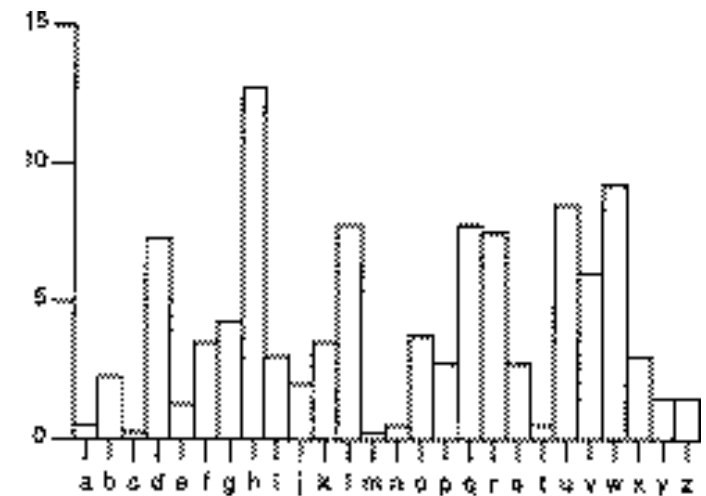


Figure 3.2 Encryption character frequencies with $i \rightarrow i+3$

Kerckhoffův princip

- A. Kerckhoffs byl holandský kryptolog v 19. století
- Bezpečnost musí záviset pouze na utajení klíče
 - Je třeba předpokládat, že útočník zná všechny podrobnosti o použitém algoritmu
- Ergo, *Security by obscurity doesn't work!*

Monoalfabetické substituční šifry

- Substituční šifry nahrazují jednotlivá písmena textu pomocí klíče, kterým je permutace všech 26 písmen (mixed alphabet).

Example: The key is a permutation:

abcdefghijklmnopqrstuvwxyz
PDUIRMFOHSBNCGVKTJWEYAQXZL

Encryption:

Plaintext: monoalphabetic substitution

Ciphertext: CVGVBNKOPDREHUWYDWEHEYEHVG

- Počet všech možných klíčů je $26! = 4 \cdot 10^{26}$
- Nerozluštitelné během celého prvního tisíciletí našeho letopočtu

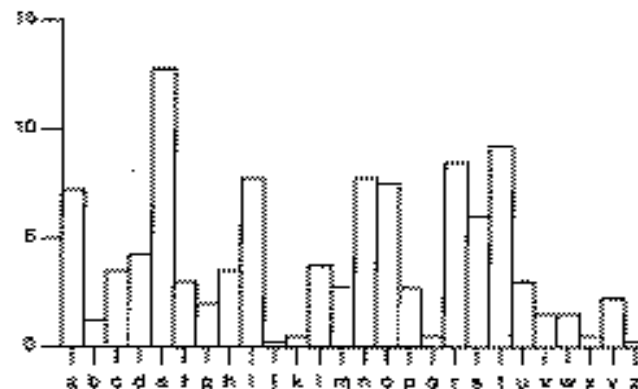
Anatomie jazyka: Frekvence

Frekvence písmen

| | | | | | |
|---|--------|---|-------|---|-------|
| e | 12.31% | l | 4.03% | b | 1.62% |
| t | 9.59 | d | 3.65 | g | 1.61 |
| a | 8.05 | c | 3.20 | v | 0.93 |
| o | 7.94 | u | 3.10 | k | 0.52 |
| n | 7.19 | p | 2.29 | q | 0.20 |
| i | 7.18 | f | 2.28 | x | 0.20 |
| s | 6.59 | m | 2.25 | j | 0.10 |
| r | 6.03 | w | 2.03 | z | 0.09 |
| h | 5.14 | y | 1.88 | | |

Frekvence slov

| | | | |
|-----|--------|------|--------|
| the | 6.421% | that | 1.244% |
| of | 4.028% | is | 1.034% |
| and | 3.150% | i | 0.945% |
| to | 2.367% | it | 0.930% |
| a | 2.091% | for | 0.770% |
| in | 1.778% | as | 0.764% |



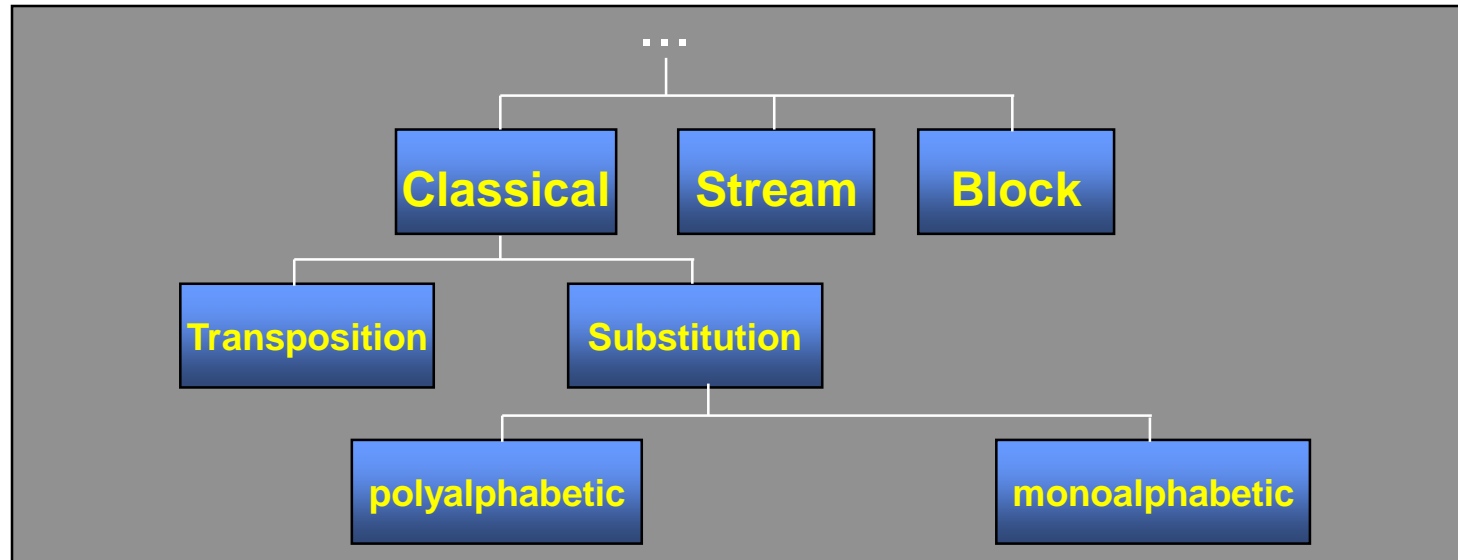
Frekvence je invariantní vzhledem k monoalfabetické substituci

Kódová kniha - Codebook

- Monoalfabetická polygramová (často homofonní) šifra
- Ukázka kódové knihy (písmeno K)
 - at 5003
 - attack 1701
 - begins 7803
 - the 3243
- plaintext: The attack begins at ...
- ciphertext: 3243 1701 7803 5003 ...
- Např. Zimmermannův telegram

Polyalfabetická substituce

- Použití více různých substitucí
- Každý znak je zašifrován jinou substituční funkcí
- Zploštění frekvenční charakteristiky jazyka
- Frekvenční analýzu ani jiné statistické metody nelze použít



Vigenerova šifra

- **Blaise de Vigenère, ~1550**
- **Nerozlomitelná cca 300 let**
- **Používá Caesarova principu**
 - s rozdílnými posuvy pro jednotlivé znaky, aby se zakryla frekvence znaků
 - znaky klíče definují posuv pro jednotlivá písmena
 - klíč je periodicky opakován, aby obsáhl celou délku šifrovaného textu

- **Příklad:**

| | |
|-----------------|-----------------|
| Otevřený text: | vigenerescipher |
| Klíč: | keykeykeykeykey |
| Šifrovaný text: | FMEORCBIQMMNRIP |

- $a=0, b=1, c=2, \dots z=25 \text{ mod } 26$

- **Vigenerova tabulka**

Vigenerova tabulka

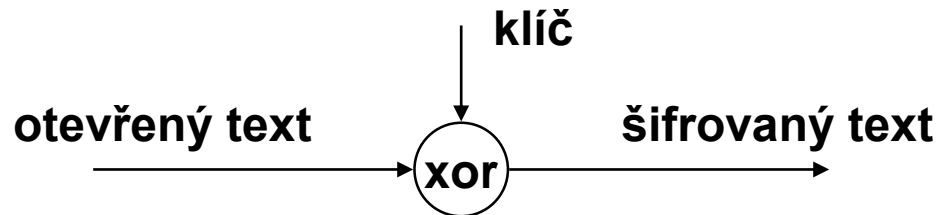
| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T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

Vigenerova šifra (útok)

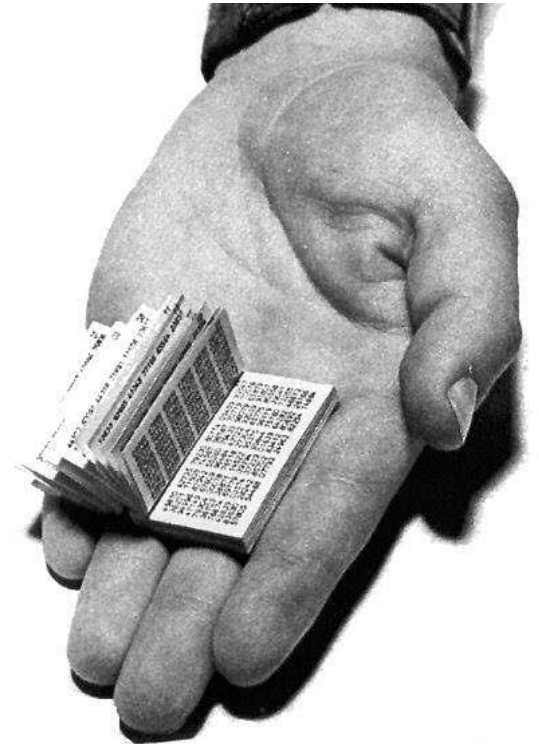
- Rozluštěna Charlesem Babbagem, ale postup byl utajován
- Nezávisle rozluštěna Friedrichem Kasiskim, 1863.
- **1. Nalezni délku klíče k**
 - pro krátký klíč zkus 1, 2, 3, ..., nebo
 - vytvoř tabulku všech vzdáleností stejných znaků v zašifrovaném textu
 - gcd nejčastějších vzdáleností je délka klíče
- **2. Nalezni písmena klíče jedno po druhém**
 - rozděl zprávu na k menších zpráv, z nichž každá obsahuje znaky, šifrované stejným písmenem klíče
 - řeš šifru jako k zpráv, zašifrovaných Caesarovou šifrou

Vernamova šifra

- One Time Pad
- Polyalfabetická substituce bez opakování klíče
- Objevena Gilbertem Vernamem z AT&T v roce 1917 pro šifrování telegrafních zpráv

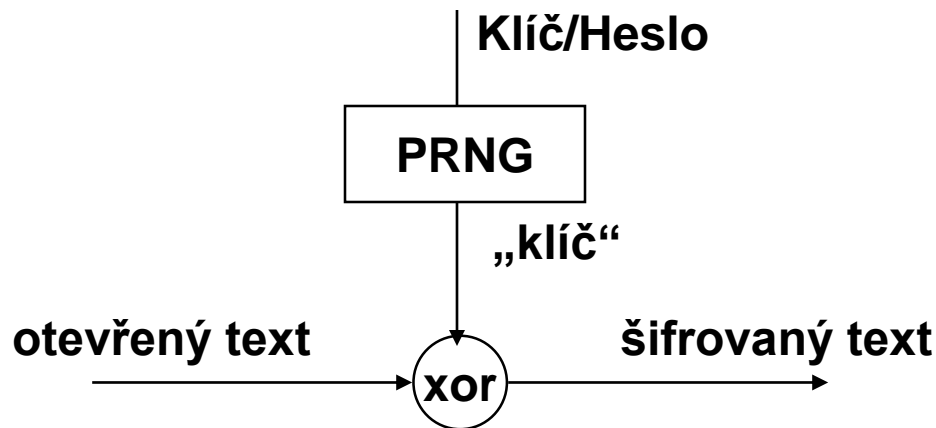


- Šifra je nerozluštitelná, pokud:
 - Klíč má stejnou délku jako všechny šifrované zprávy
 - Klíč se nikdy nepoužije znovu
 - Klíč je náhodně zvolen (opravdu náhodně)



Co NENÍ Vernamova šifra

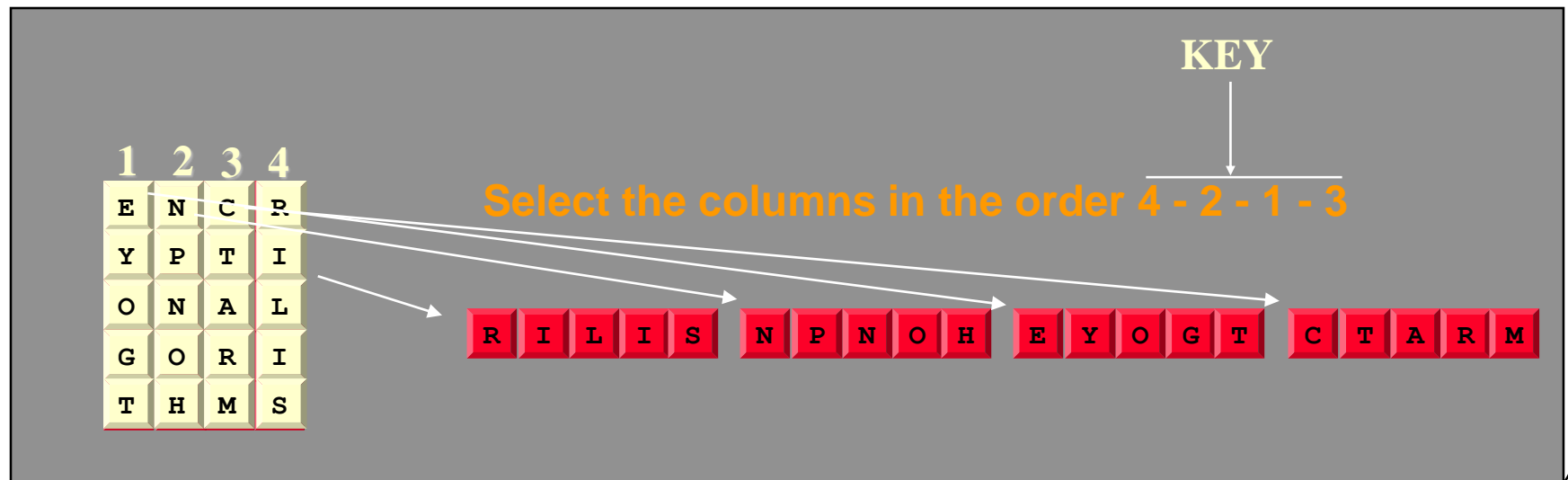
- Nekonečný klíč se vyrobí z konečného klíče/hesla (např. o délce 128 bitů) pomocí generátoru pseudonáhodné posloupnosti (PRNG)
- Tento princip se často nazývá „proudová šifra“
- Klíč nesplňuje požadavek dostatečné délky pro Vernamovu šifru



Sloupcová transpozice

Columnar Transposition

- Zpráva se zapíše po řádcích a šifrovaný text se vytvoří tak, že se čte po sloupcích v daném pořadí
- Např. zpráva je “encryption algorithms”, matice je 5x4 a klíč je 4 - 2 - 1 - 3



Složené šifry - Product Ciphers

- Jedna šifra (substituční nebo transpoziční) se nejevila dostatečně bezpečná
- Nabízí se zašifrovat zprávu postupně několika šiframi, ale
 - Dvě substituce za sebou tvoří jenom jednu (složitější) substituci
 - Dvě transpozice za sebou tvoří jenom jednu (složitější) transpozici
 - Ale substituce následovaná transpozicí vytvoří novou, bezpečnější šifru
- Složené šifry se obvykle skládají z kombinací substitucí a transpozicí
- Pro ruční realizaci dost komplikovaná, ale používala se
- Pro mechanický stroj také příliš komplikovaná
- Princip se ale používá v moderní kryptografii

Posouvané a rotované abecedy

- **Založené na jednoduché substituci**
 - Horizontálně posouvaná abeceda
 - Vertikálně posouvaná abeceda
 - » Vertikálně pokračovaná ve standardním pořadí
 - Rotovaná abeceda
 - » Diagonálně pokračovaná ve standardním pořadí

| | |
|---|----------------------------|
| i | abcdefghijklmnopqrstuvwxyz |
|---|----------------------------|

| | |
|---|----------------------------|
| 0 | NEWYORKCITABDFGHJLMPQSUVXZ |
|---|----------------------------|

| | |
|---|----------------------------|
| 1 | EWYORKCITABDFGHJLMPQSUVXZN |
|---|----------------------------|

| | |
|---|----------------------------|
| 2 | WYORKCITABDFGHJLMPQSUVXZNE |
|---|----------------------------|

| | |
|---|----------------------------|
| i | abcdefghijklmnopqrstuvwxyz |
|---|----------------------------|

| | |
|---|----------------------------|
| 0 | NEWYORKCITABDFGHJLMPQSUVXZ |
|---|----------------------------|

| | |
|---|----------------------------|
| 1 | OFXZPSLDJUBCEGHIKMNQRTUWYA |
|---|----------------------------|

| | |
|---|----------------------------|
| 2 | PGYAQTMEKVCDFHIJLNORSUVXZB |
|---|----------------------------|

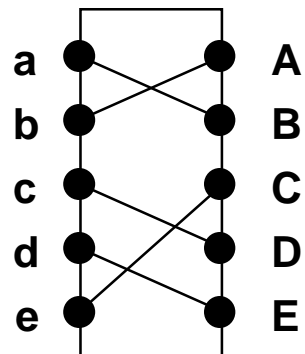
| | |
|---|----------------------------|
| i | abcdefghijklmnopqrstuvwxyz |
|---|----------------------------|

| | |
|---|----------------------------|
| 0 | NEWYORKCITABDFGHJLMPQSUVXZ |
|---|----------------------------|

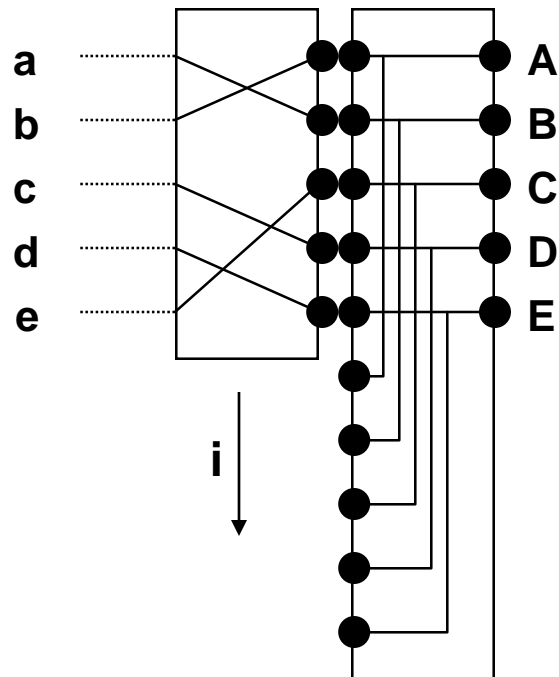
| | |
|---|----------------------------|
| 1 | AOFXZPSIDJUBCEGHIKMNQRTVWY |
|---|----------------------------|

| | |
|---|----------------------------|
| 2 | ZBPGYAQTJEKVCDFHIJLNORSUWZ |
|---|----------------------------|

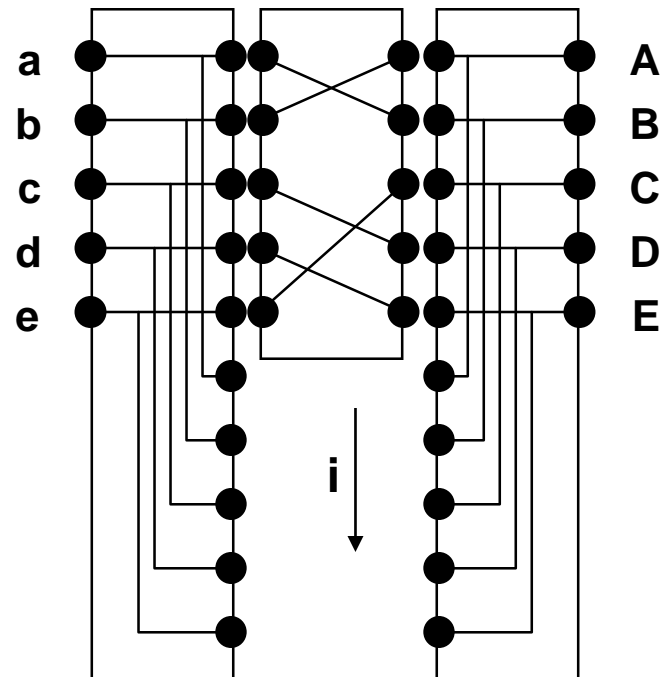
Stroje pro posouvání abecedy



Substitute



Vertikální posuv



Rotace

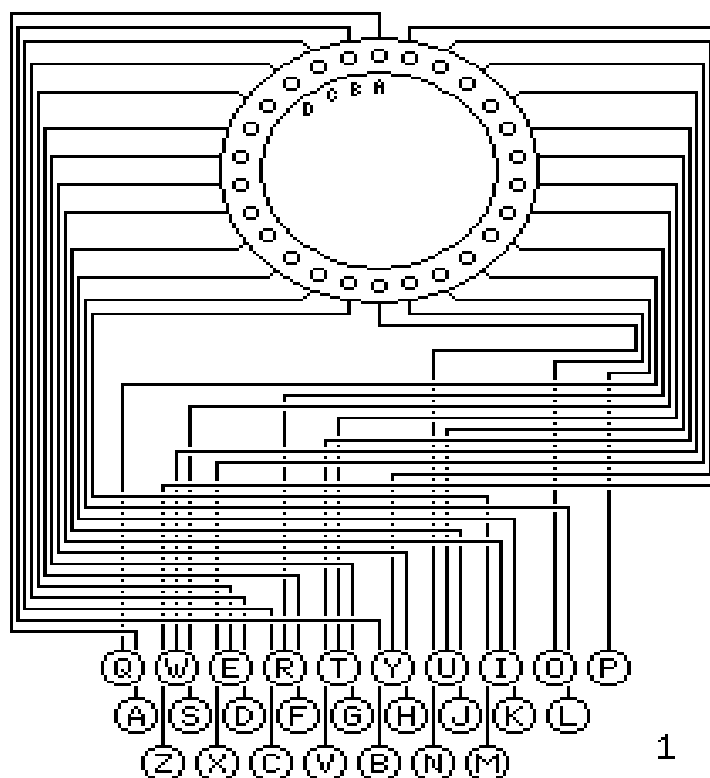
Rotorové stroje

- Implementují polyalfabetické substituční šifry s dlouhou periodou pomocí sady rotorů
- Každý rotor má 26 kontaktů na obou stranách. Kontakty z přední strany jsou propojeny s kontakty ze zadní strany. Klíč je dán propojením kontaktů a počáteční pozicí rotorů.

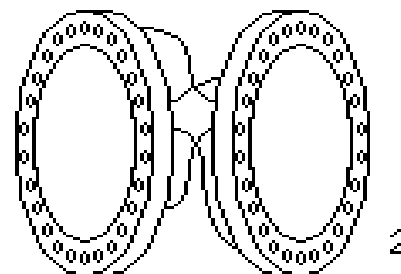


Rotorové stroje

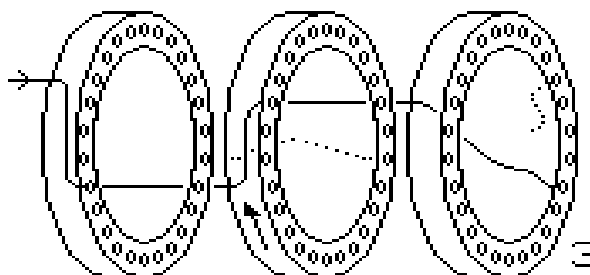
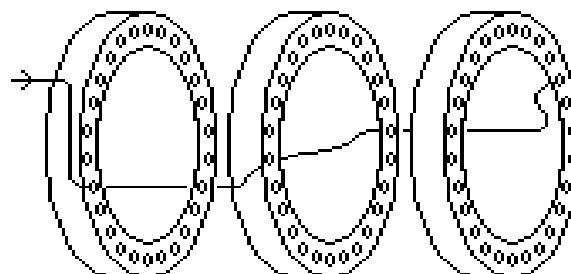
- Otevřený text vstupuje do sady rotorů na jedné straně a vystupuje zašifrovaný na druhé straně.
- Po zašifrování písmene se pootočí jeden nebo více rotorů.



1



2



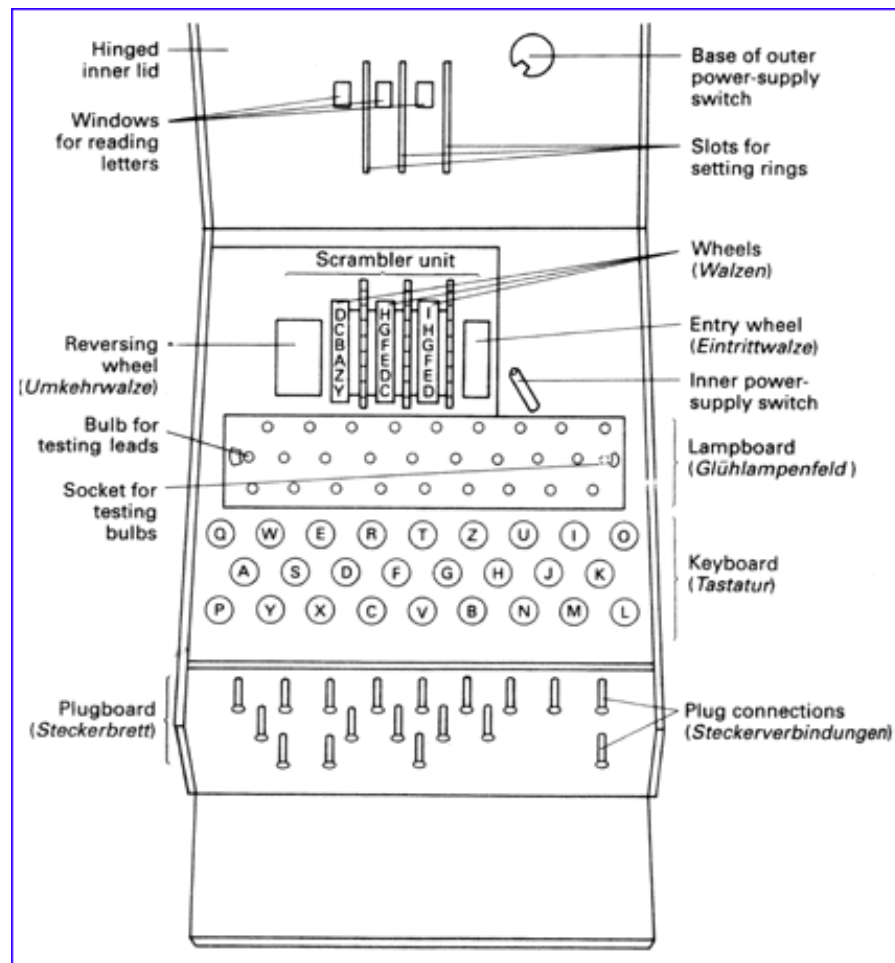
3

Enigma



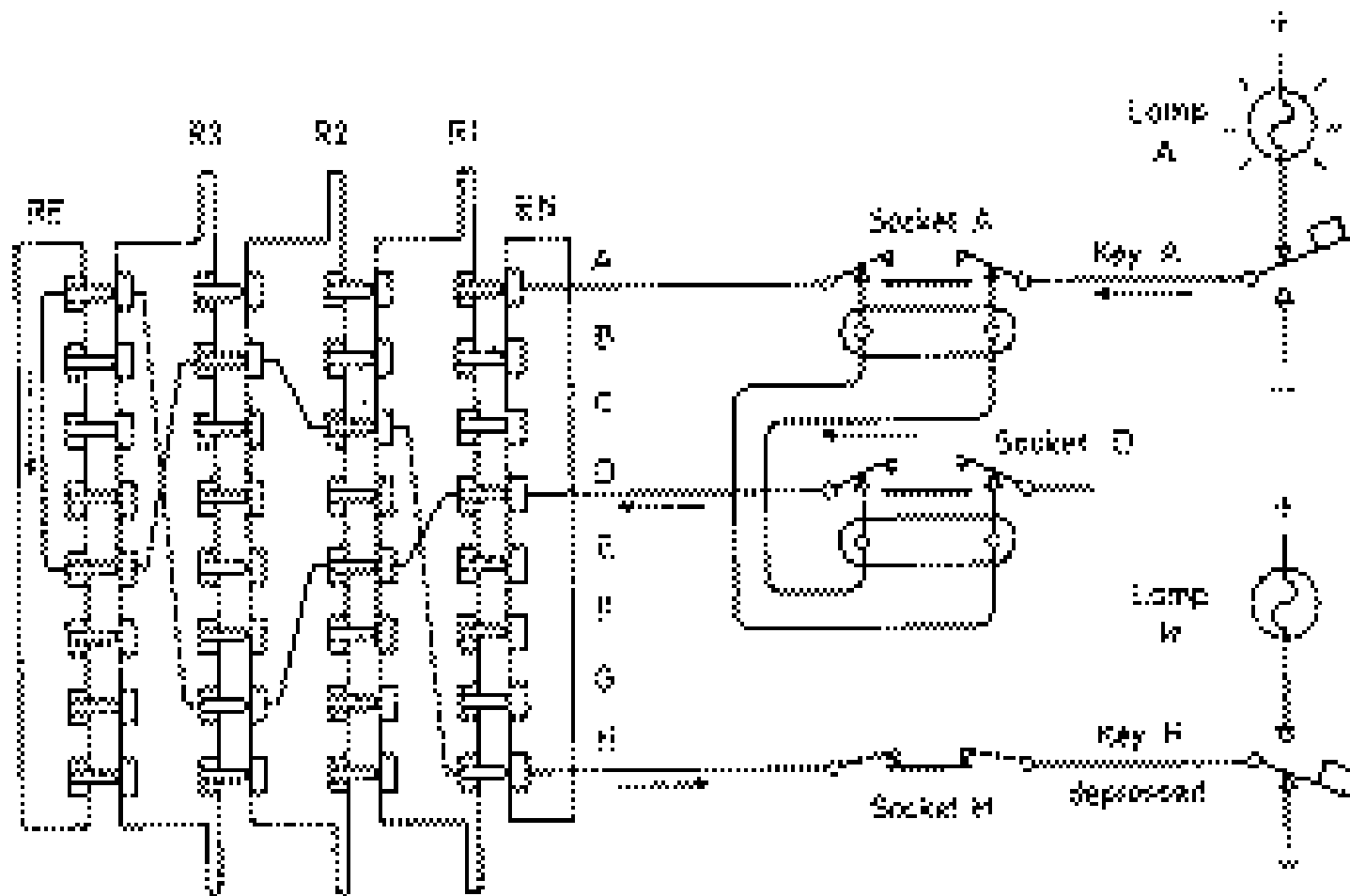
- **Vytvořena pro komerční účely 1923**
- **Upravena pro Wehrmacht**
- **Cca. 50000 kusů**
- **V průběhu války modifikována, pokládána za zcela bezpečnou**

Enigma



- **Tři rotory (vybrány z pěti možných)**
- **Po každém znaku se první rotor pootočí**
- **Po dojetí na zarážku se pootočí další rotor**
- **Reflektor**
- **Propojovací deska (Plugboard, Steckerbrett)**

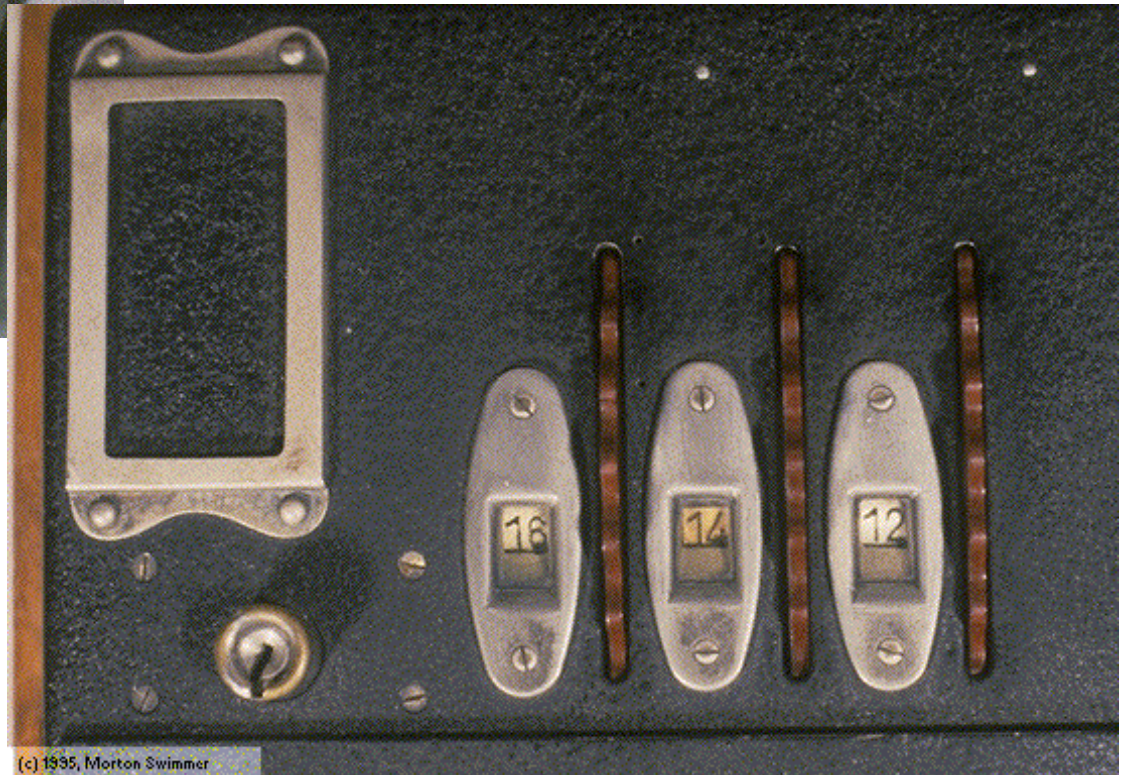
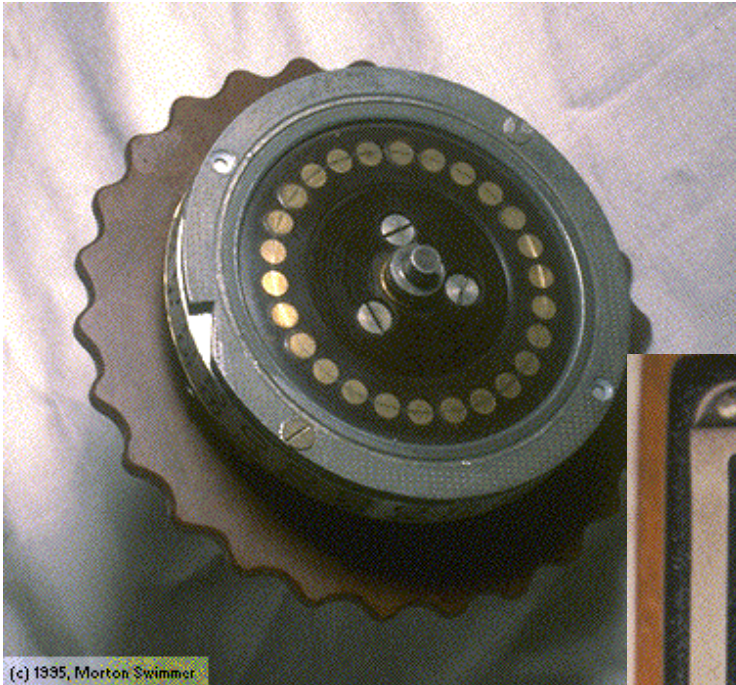
S propojovací deskou



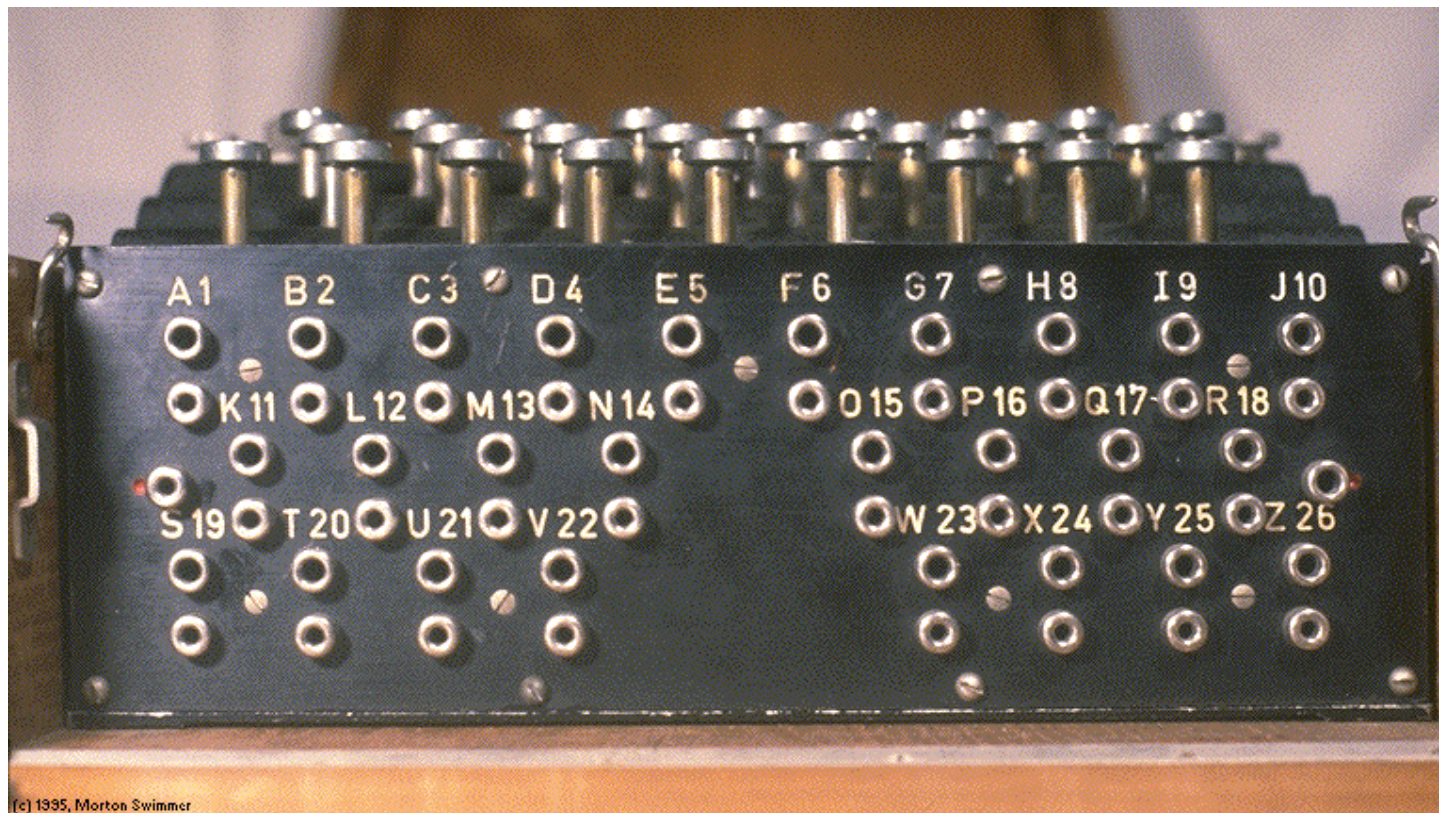
Enigma: Klávesnice a displej



Enigma: Rotary



Enigma: Propojovací deska



Nastavení (klíč)

- **Rotory**
 - **Walzenlage**
 - » Před rokem 1939 – Tři rotory (ze tří možných)
 - » Později - Tři rotory (z pěti možných)
 - **Grundstellung**
 - » Počáteční orientace tří rotorů
 - **Ringstellung**
 - » „Posunutí“ počáteční orientace rotorů
 - » Nastavení, kdy se pootočí další rotor
- **Propojovací deska**
 - **Steckerverbindung**
 - » Výměna páru znaků pomocí kabelu
 - » Počet kabelů se měnil (≤ 6 do roku 1939, později až 10)

Počet možných klíčů

- Pokud útočník nezná propojení rotorů:

$$(26!)^3 \approx 4 * 10^{26}$$

- Pokud útočník nezná propojení reflektoru:

$$(26 * 25 / 2) * (24 * 23 / 2) * \dots * (2 * 2) / 13! \\ \approx 8 * 10^{12}$$

- Propojovací deska se šesti kabely:

$$(26 * 25/2) * \dots * (16*15 / 2) / 6! \approx 10^{11}$$

- Ringstellung: $26^2 = 676$
- Grundstellung: $26^3 = 17576$
- Celkem: $\approx 6 * 10^{110}$

(ve vesmíru je 10^{84} atomů)

Útočník ukořistí jeden stroj

- Pokud útočník nezná propojení rotorů:

$$(26!)^3 \approx 4 * 10^{26}$$

Znamé rotory:

$$3! = 6$$

Nebo $3 \text{ z } 5 = 5 * 4 * 3 = 60$

- Pokud útočník nezná propojení reflektoru:

$$(26 * 25 / 2) * (24 * 23 / 2) * \dots * (2 * 2) / 13! \\ \approx 8 * 10^{12}$$

Znamý reflektor: 1

- Propojovací deska se šesti kabely:

$$(26 * 25/2) * \dots * (16*15 / 2) / 6! \approx 10^{11}$$

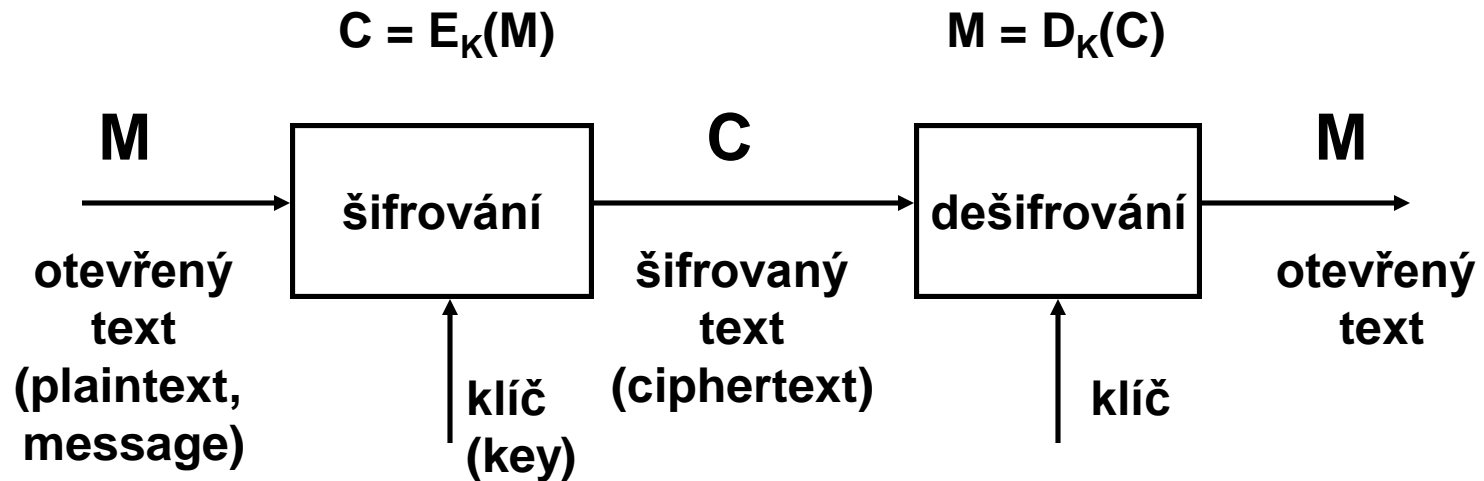
- Ringstellung: $26^2 = 676$
- Grundstellung: $26^3 = 17576$
- Celkem: $\approx 10^{16}$



Moderní kryptografie

Petr Hanáček
Faculty of Information Technology
Technical University of Brno
Božetěchova 2
612 66 Brno
tel. (05) 4114 1216
e-mail: hanacek@fit.vutbr.cz

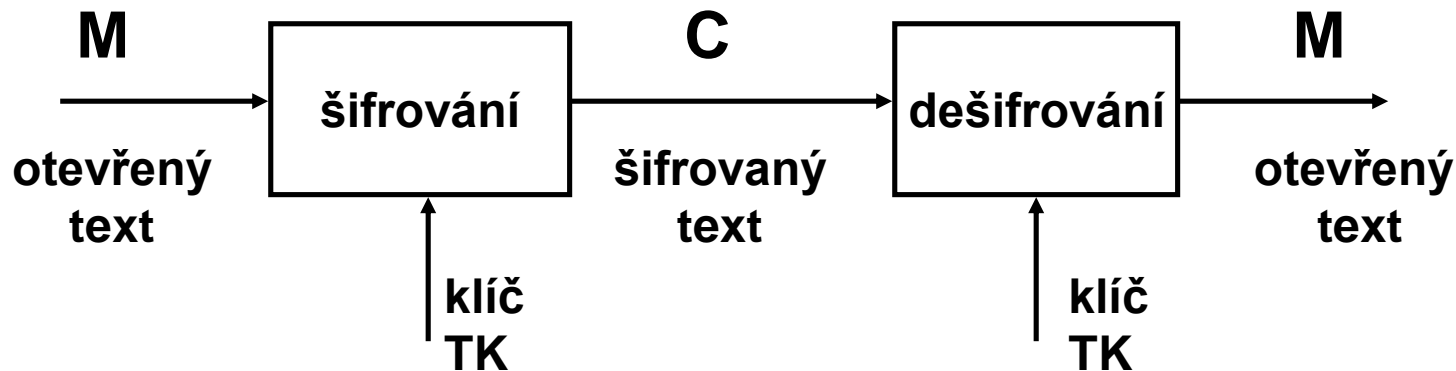
Kryptografie



- **podle klíčů**

- symetrické X asymetrické
- tajný klíč X veřejný klíč, soukromý klíč

Symetrický algoritmus



- **S tajným klíčem**
 - Uživatelé se dohodnou na stejném tajném klíči
 - Sdílené tajemství
- **Útoky (COA, KPA)**
- **„Bezpečný algoritmus“**
- **Útok silou**

Důvěrnost
Autentizace
Integrita
Nepopiratelnost

Útok silou

| • Délka klíče | 1 test / uS | 10^6 procesorů |
|---------------|-------------|------------------|
| 32 | 35.8 m | 2.15 ms |
| 40 | 6.4 d | 550 ms |
| 48 | 4.46 r | 2.35 m |
| 56 | >100 r | 10.0 h |
| 64 | | 107 d |

Typy útoků

- 1 počítač
- Paralelní superpočítač
- Celý svět (Čínská loterie)

Reálné útoky silou

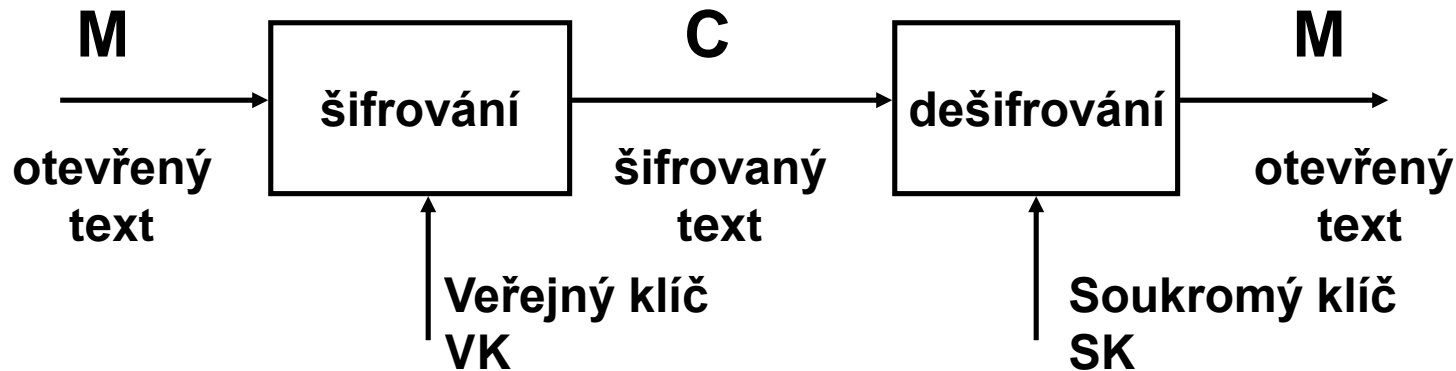
| Date | Key length | Time | # Computers | Rate (keys/sec) |
|------|------------|-----------|--------------------|-----------------|
| 8/95 | 40 | 8 days | 120 + 2 super | 0.5 M |
| 1/97 | 40 | 3.5 hours | 250 | 27 M |
| 2/97 | 48 | 13 days | 3,500 | 440 M |
| 6/97 | 56 | 4 months | 78,000 | 7 B |
| 2/98 | 56 | 39 days | 22,000 people | 34 B |
| 7/98 | 56 | 56 hours | 1 with 1,728 chips | 90 B |
| 1/99 | 56 | 22 hours | 100,000 + 1 | 250 B |

Symetrické algoritmy

- DES – 56 bit
- 3DES – 112 bit
- IDEA – 128-bit keys, PGP used in early versions
- RC2 – “Ron’s code” (Ron Rivest), variable size key
- RC5 – variable size key
- Skipjack – 80-bit key, 32 rounds, NSA initially classified
- AES – variable size key

- Možnost vytvořit nový

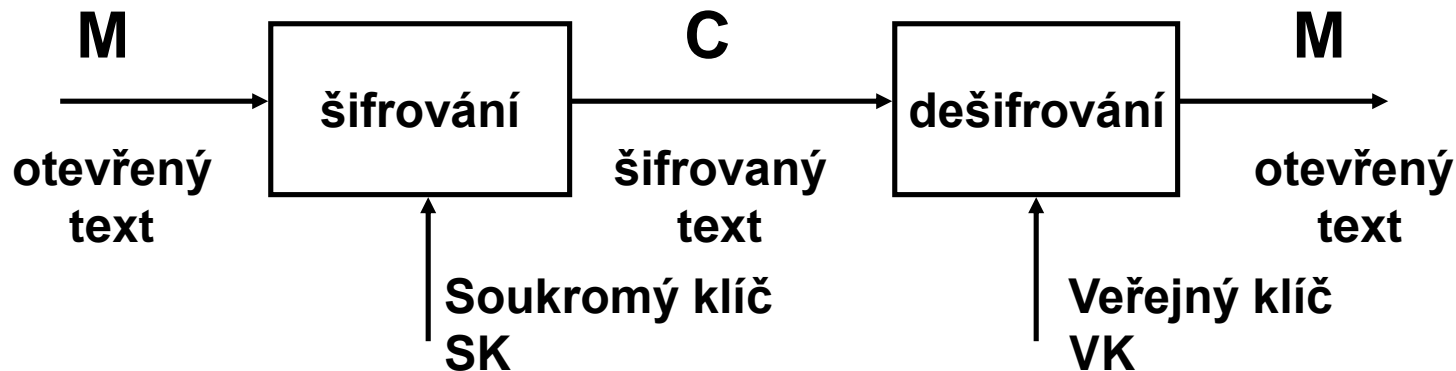
Asymetrický algoritmus 1



- **Uživatel tají soukromý klíč, zveřejní veřejný klíč**

Důvěrnost
Autentizace
Integrita
Nepopiratelnost

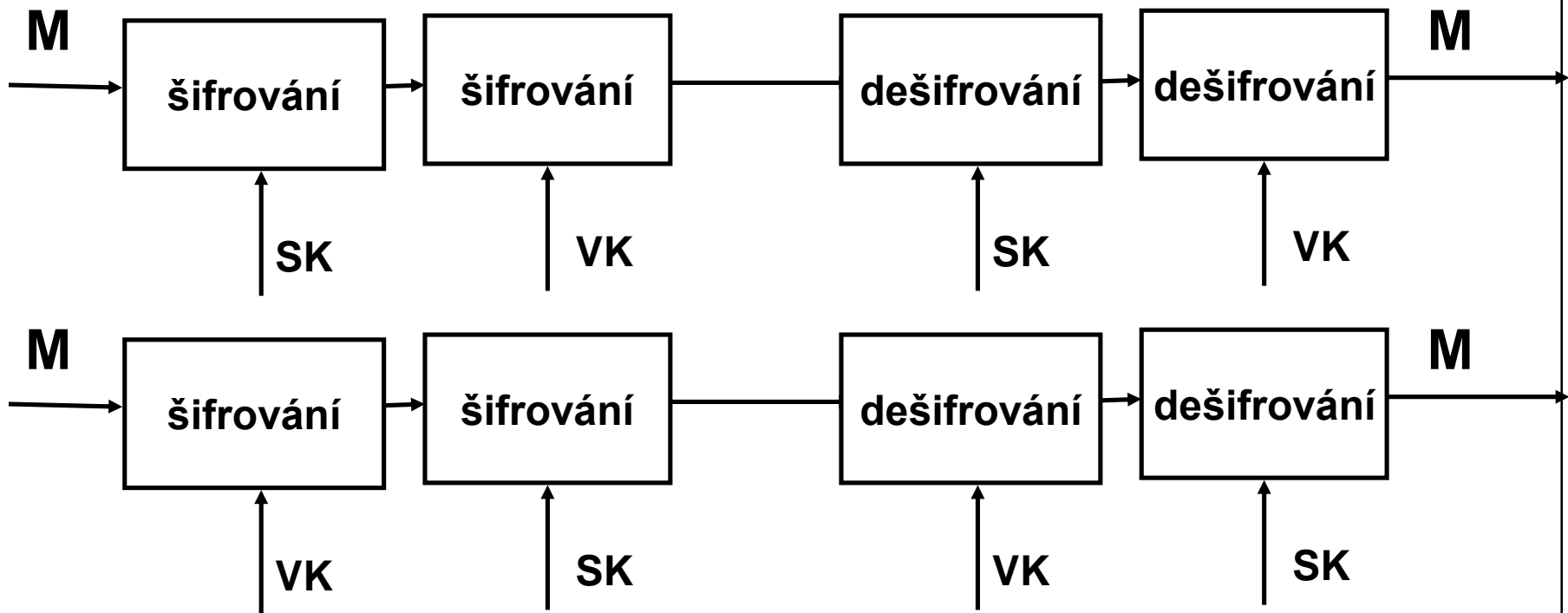
Asymetrický algoritmus 2



- Uživatel tají soukromý klíč, zveřejní veřejný klíč
- Elektronický podpis

Důvěrnost
Autentizace
Integrita
Nepopiratelnost

Asymetrický algoritmus 3



- Pořadí ?

Důvěrnost
Autentizace
Integrita
Nepopiratelnost

Asymetrické algoritmy

- RSA (Rivest – Shamir - Adleman)
- DSS/DSA (Digital Signature Standard)
- DH (Diffie-Hellman)
- Knapsack
- EC – Elliptic Curves

- Délky klíčů – 768, 1024, 2048 bitů
- Nemožnost vytvořit nový

Knapsack
Faktorizace čísel
Diskrétní logaritmus
Eliptické křivky

Porovnání vlastností

| • . | Tajný klíč | Veřejný klíč |
|-----------------------|------------|--------------|
| kopíí / tajemství | 2 | 1 |
| tajemství / uživatelé | mnoho | 1 |
| rozšiřovatelnost | špatná | dobrá |
| rychlost | dobrá | malá |

Hašovací funkce

- Hašovací funkce, charakteristika zprávy, jednocestná funkce, message digest, digest, hash, hash function, one way function
- je to funkce F taková, že
 - je aplikovatelná na argument libovolné velikosti
 - její výstupní hodnota má konstantní délku (zpravidla 128, 160 nebo 256 bitů)
 - lze rychle spočítat $F(x)$
 - pro dané y je výpočetně nezvládnutelné nalézt takové x , aby platilo $F(x)=y$ (*first preimage resistance*)
 - pro dané x je výpočetně nezvládnutelné nalézt takové $x' \neq x$, aby platilo $F(x')=F(x)$ (*second preimage resistance*)
 - je výpočetně nezvládnutelné nalézt takové x' a x , $x' \neq x$, aby platilo $F(x')=F(x)$ (*collision resistance*)
- implementace
 - MD2, MD4, MD5
 - SHS (Secure Hash Standard), SHA

Birthday attack

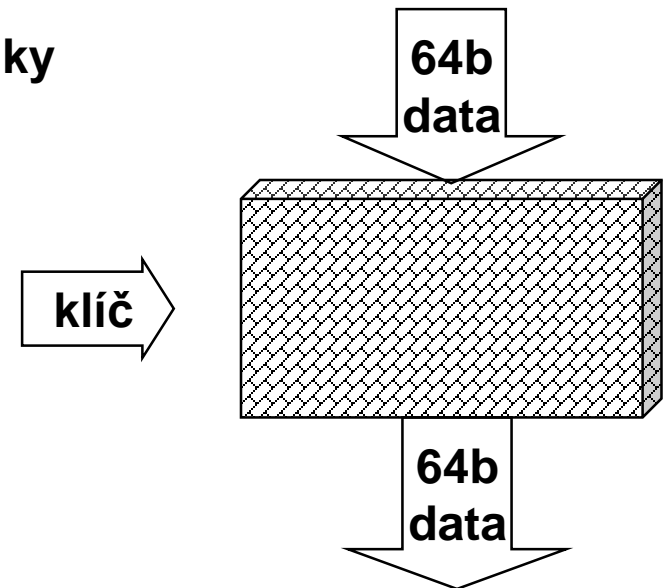
- Birthday paradox:
 $r_1, \dots, r_n \in [0, 1, \dots, B]$ indep. random integers.
When $n = 1.2 \sqrt{B}$ then
$$\Pr[\exists i \neq j : r_i = r_j] > \frac{1}{2}$$
- msg-digest only 64 bits long \Rightarrow
can find collision in 2^{32} tries.
- Typical digest size = 160 bits. (e.g. SHA-1)
 \Rightarrow collision time is 2^{80} tries.

Základní schéma

Blokové šifry a DES

Bloková šifra

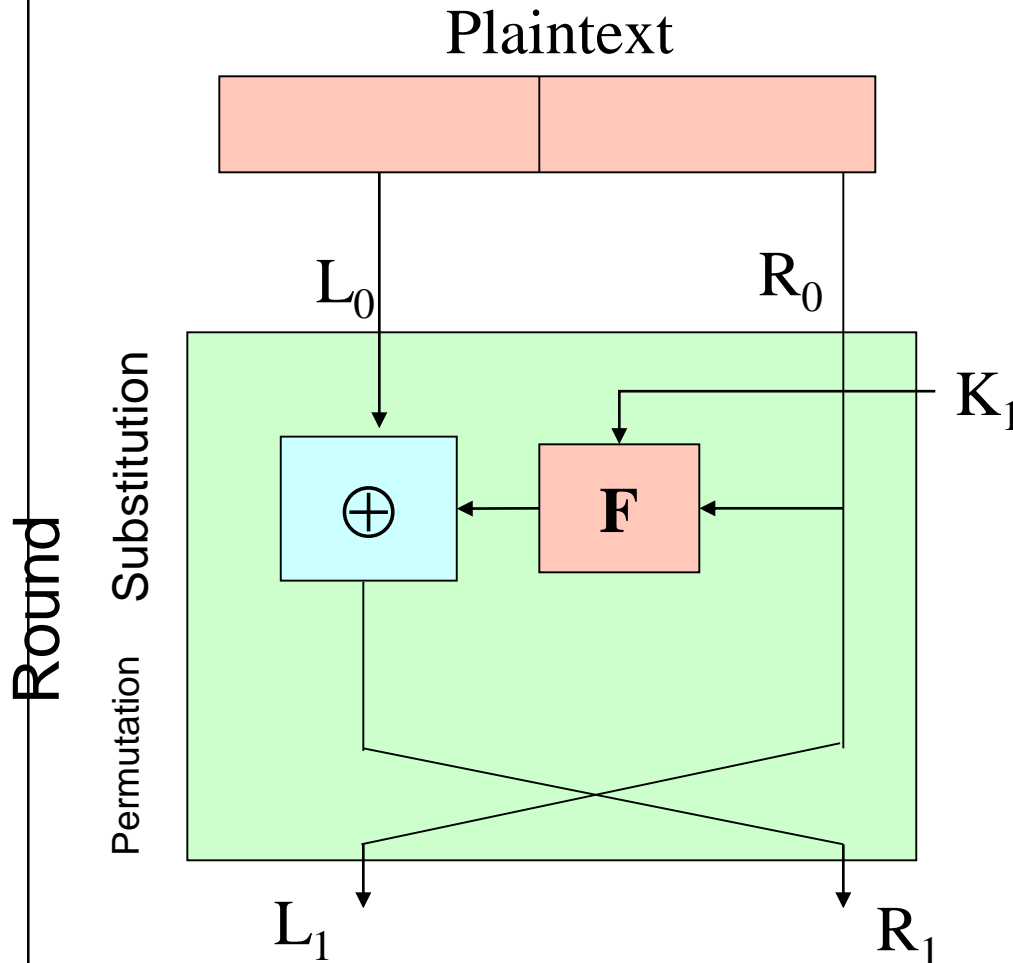
- 64 bitové bloky dat (nyní 128 až 256)
- 2^{64} možných bloků otevřeného textu, alespoň 2^{64} odpovídajících bloků zašifrovaného textu
 - Existuje $2^{64}!$ možných zobrazení
- Proč nevytvořit náhodné zobrazení?
 - Byla by třeba $2^{64} * 64$ -bitová tabulka $\approx 10^{21}$ bitů
 - \$14 quadrillion
 - Přenos klíče znamená přenos nové tabulky
- Ideální náhodné zobrazení aproximujeme pomocí několika komponent, řízených hodnotou klíče



Feistelova šifra

- Základ některých symetrických šifer
 - Horst Feistel pracoval pro IBM v roce 1973
 - IBM's *Lucifer* algoritmus, založený na Feistelově principu, byl základem pro algoritmus DES v roce 1977
- Mnoho jiných algoritmů používá Feistelův princip
- Mimo Feistelův princip jsou však i jiné iterativní principy

Feistelova šifra



L_0 = left half of plaintext

R_0 = right half of plaintext

$$L_i = R_{i-1}$$

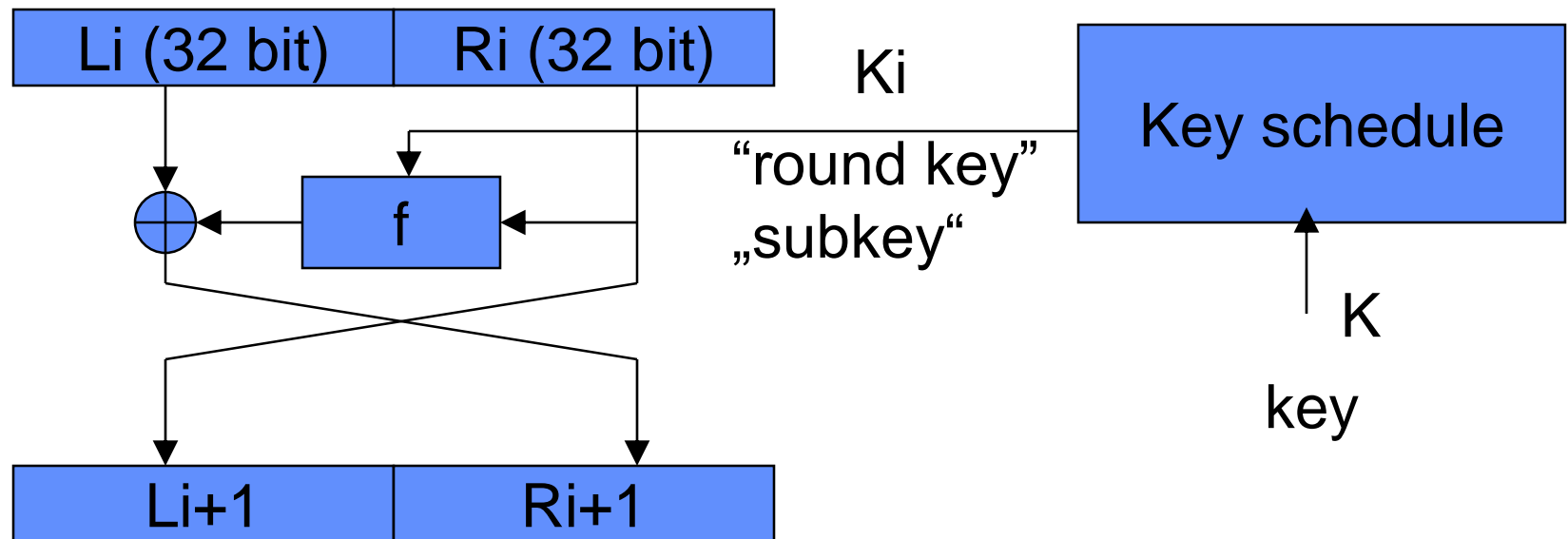
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

$$C = R_n \parallel L_n$$

n is number of rounds
(undo last permutation)

Subklíče

- Vytvářejí se v bloku “Key schedule”
- Tvorba subklíčů má velmi výrazný vliv na bezpečnost algoritmu
 - Možnost vytvoření slabých subklíčů („00000000“ ??)
 - Možnost slabých klíčů



DES

Algoritmus DES

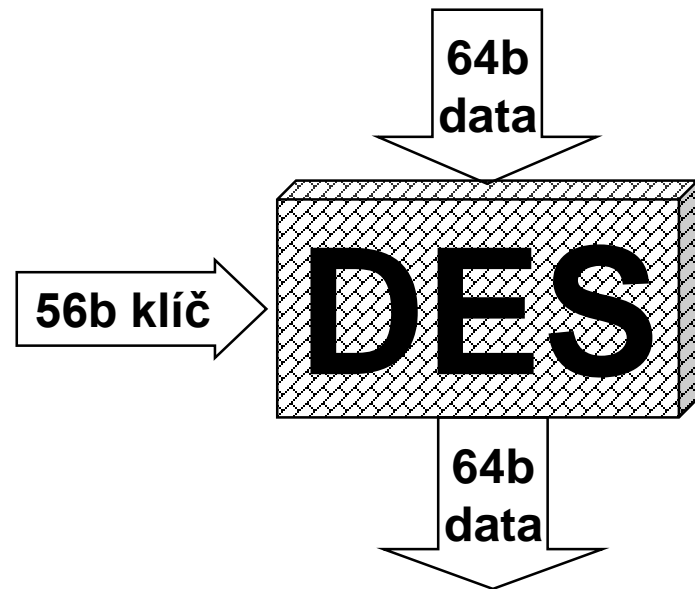
- vyvinut IBM v r. 1976 na zakázku NBS (nyní NIST)
- Na základě algoritmu Lucifer od IBM
- Modifikován NSA
 - Změna S-Boxů
 - Redukovaná délka klíče ze 128 na 56 bitů
- Přijat jako standard v r. 1976
- Zašifroval nejvíce bitů ze všech algoritmů

Požadavky na DES

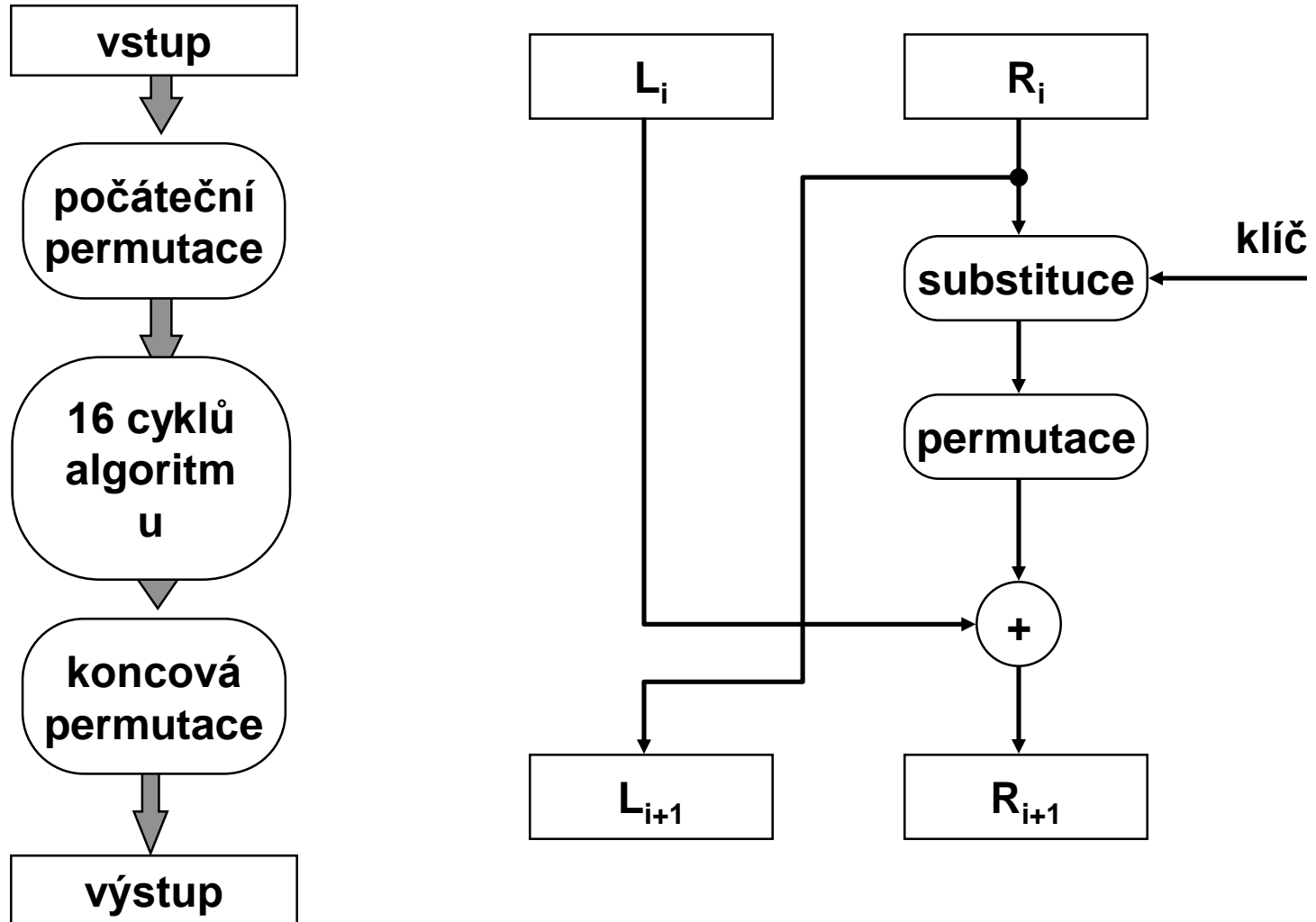
- musí zajišťovat vysokou bezpečnost
- musí být přesně specifikovaný
- bezpečnost nesmí záviset na utajení algoritmu
- musí být realizovatelný pomocí hardware
- musí být rychlý

DES

- symetrický šifrovací algoritmus tajným klíčem
- šifruje bloky dat o šířce 64 bitů klíčem o velikosti 56 bitů
- Feistelova šifra s dodatečnou počáteční permutací IP
- Komplikovaná funkce F
- 16 kol
- 56-bitový klíč, posuvy a permutace vytvářejí 48-bitové subklíče pro každé kolo



DES



DES - slabiny a pochybnosti

- **Velikost bloku a klíče**
 - Je více bloků než klíčů
 - Pro jeden blok 2^{64} zpráv $> 2^{56}$ klíčů
 - Zašifrovaný konstantí blok nemůže nabýt všech 2^{64} možných hodnot
- **56-bitový klíč je příliš krátký**
 - vedou se úvahy o případné úspěšnosti útoku silou
- **Komplementární klíče**
- **Mezi klíči existují tzv. slabé klíče**
 - při generování klíče je třeba kontrolovat, zda nejde o slabý nebo poloslabý klíč
- **Návrh S-boxů nebyl zveřejněn - možnost “zadních vrátek”**
 - pokud by S-boxy byly nějakou lineární funkcí, autor S-boxů může snadno šifru rozbít
- **Není zcela jasné, zda 16 cyklů je postačující pro bezpečné zašifrování**

Útoky na DES

- **Využívající slabin**
 - Slabé (poloslabé klíče)
 - Komplementární klíče (z krácení z 56 bitů na 55 bitů)
 - Diferenciální kryptoanalýza – není prakticky použitelná
 - Lineární kryptoanalýza – není prakticky použitelná
- **Útok silou**
 - Nejlepší známý útok
- 1990, Eli Biham a Adi Shamir, diferenciální kryptoanalýza
- 1993, Mitsuru Matsui, lineární kryptoanalýza

Praktické útoky silou

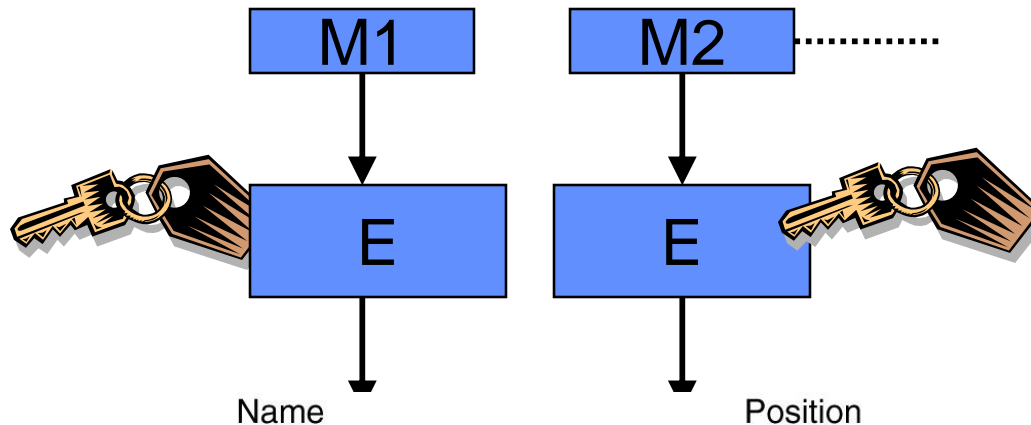
| Date | Key length | Time | # Computers | Rate (keys/sec) |
|------|------------|-----------|------------------------|-----------------|
| 8/95 | 40 | 8 days | 120 + 2 super | 0.5 M |
| 1/97 | 40 | 3.5 hours | 250 | 27 M |
| 2/97 | 48 | 13 days | 3,500 | 440 M |
| 6/97 | 56 | 4 months | 78,000 | 7 B |
| 2/98 | 56 | 39 days | 22,000 people | 34 B |
| 7/98 | 56 | 56 hours | 1 EFF with 1,728 chips | 90 B |
| 1/99 | 56 | 22 hours | 100,000 + 1 EFF | 250 B |

Režimy blokových šifer

Režimy blokových šifer

- Definovány ve FIPS PUB 81
- 4 režimy
 - Electronic Codebook (ECB)
 - Cipher Block Chaining (CBC)
 - Output Feedback (OFB)
 - Cipher Feedback (CFB)
- Mohou být použity pro jakoukoli blokovou šifru

ECB (Electronic Code Book)



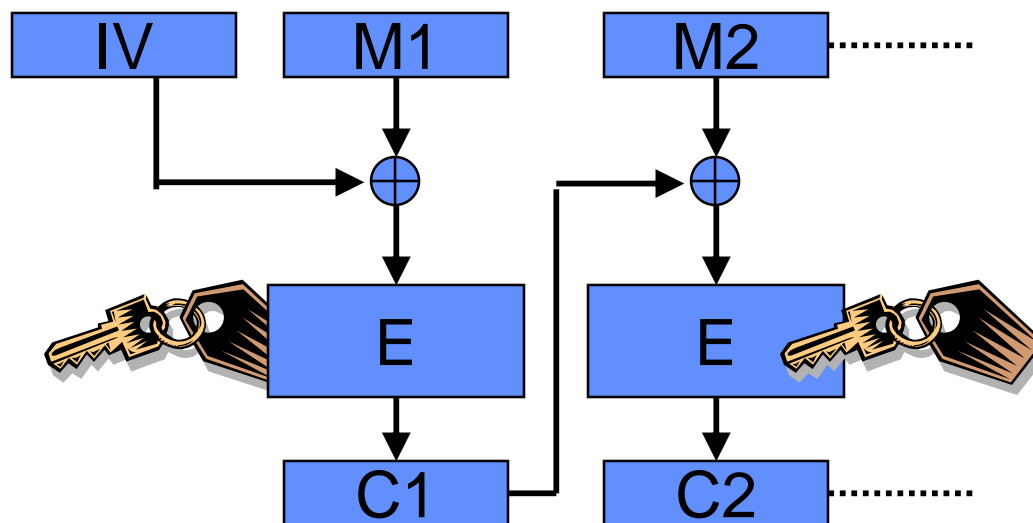
| | | | | | | | | | | |
|-----------------|-------------|---------------|----|---|---|---|---|---|---|---|
| A d a m s , | L e s l i e | C l e r k | \$ | | | | | 1 | 0 | |
| B l a c k , | R o b i n | B o s s | \$ | 5 | 0 | 0 | , | 0 | 0 | 0 |
| C o l l i n s , | K i m | M a n a g e r | \$ | 1 | 0 | 0 | , | 0 | 0 | 0 |
| D a v i s , | B o b b i e | J a n i t o r | \$ | | | | | | | 5 |

Bytes ← 16 → 8 → 8 →

- **Umožňuje**
 - Slovníkové útoky
 - Repetici bloků
 - Přeskládání bloků

Cipher Block Chaining (CBC)

- Každý blok zprávy je xorován z předchozím zašifrovaným blokem
 - $C_i = E(K, (M_i \text{ XOR } C_{i-1}))$
- První blok je xorován s inicializačním vektorem IV



Cipher Feedback (CFB)

- Ciphertext is XOR of plaintext and key stream
- DES je inicializován inicializačním vektorem IV
- Vstupní blok DESu je posunut doleva o k bitů a zprava je doplněn k bity ciphertextu
- Typicky $k = 8$ nebo 64

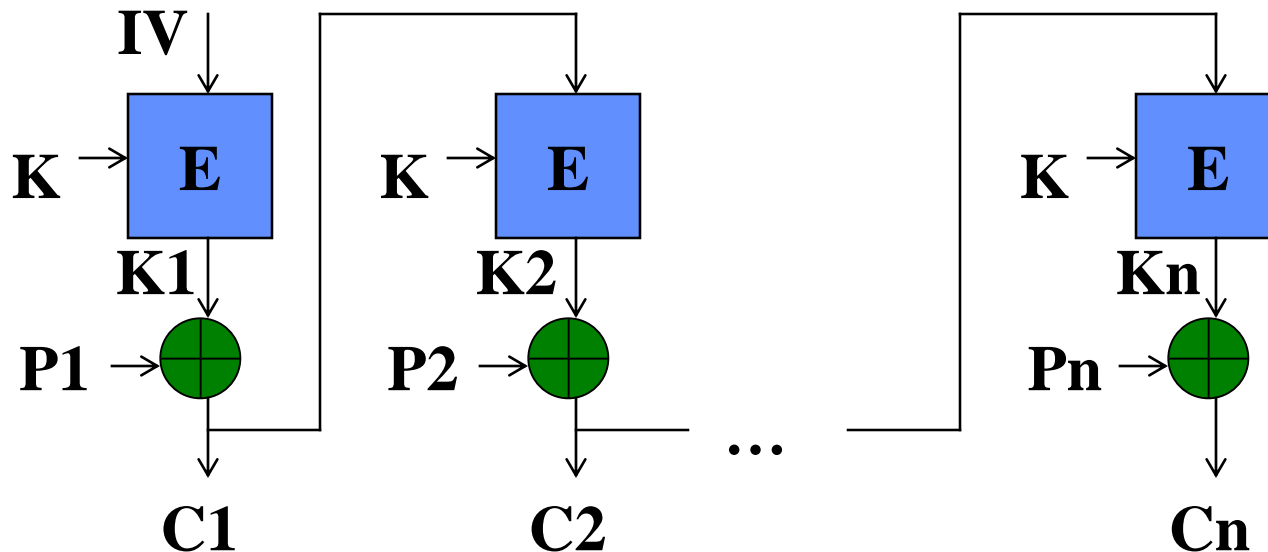
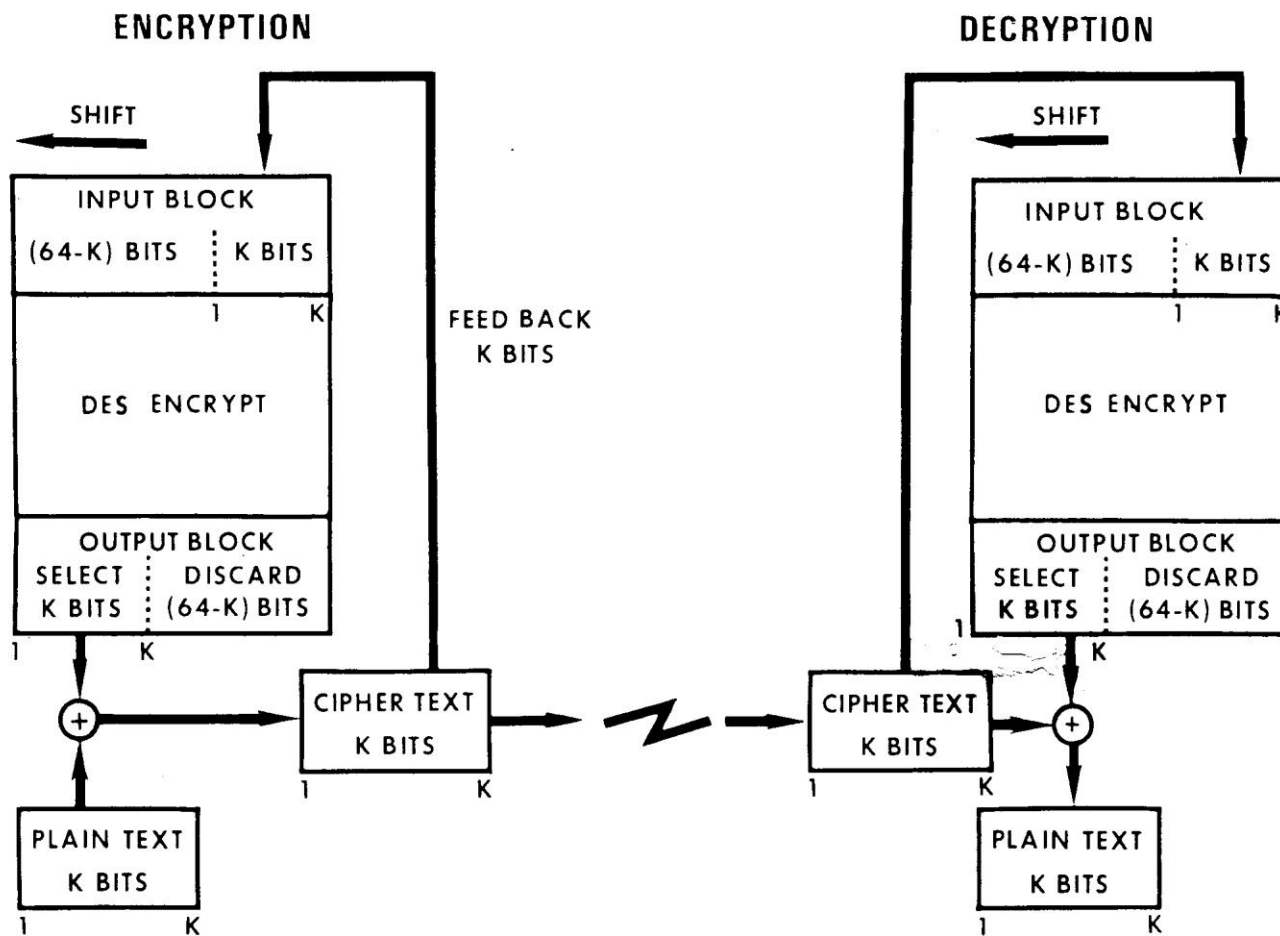


FIGURE 3: K-BIT CIPHER FEEDBACK (CFB) MODE



INPUT BLOCK INITIALLY CONTAINS AN INITIALIZATION VECTOR (IV) RIGHT JUSTIFIED.

Output Feedback (OFB)

- **Synchronní proudová šifra**
 - DES je použit pro generování pseudonáhodné posloupnosti (key stream)
- **DES je inicializován inicializačním vektorem IV**
- **Vstupní blok DESu je posunut doleva o k bitů a zprava je doplněn k bity výstupního bloku**
 - Typicky $k = 8$ nebo 64
- **Tentýž key stream nesmí být víckrát použit !**

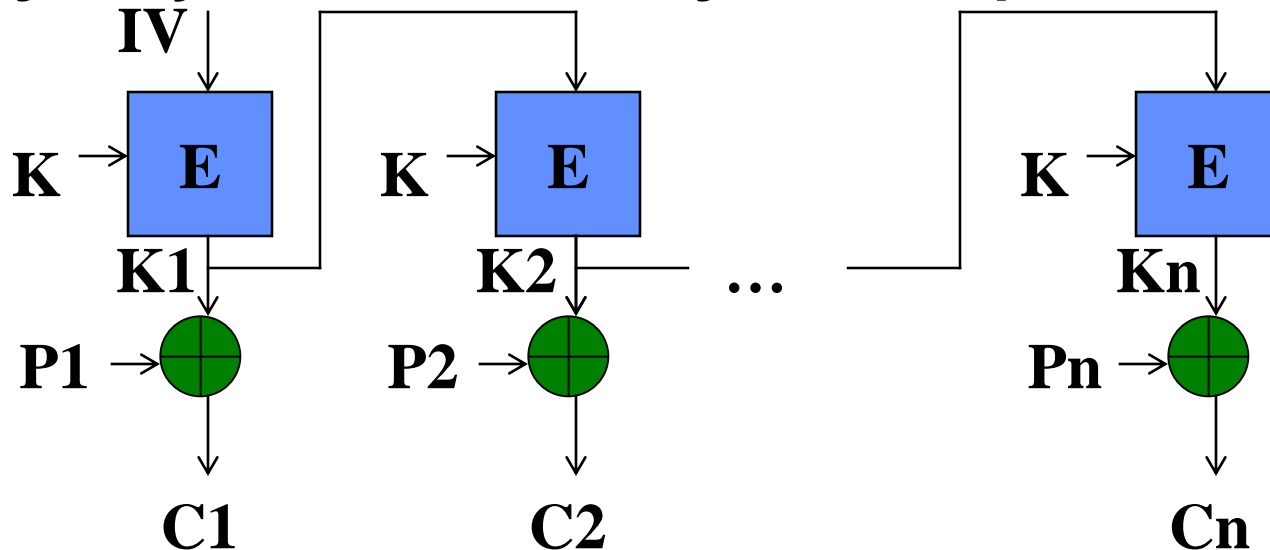
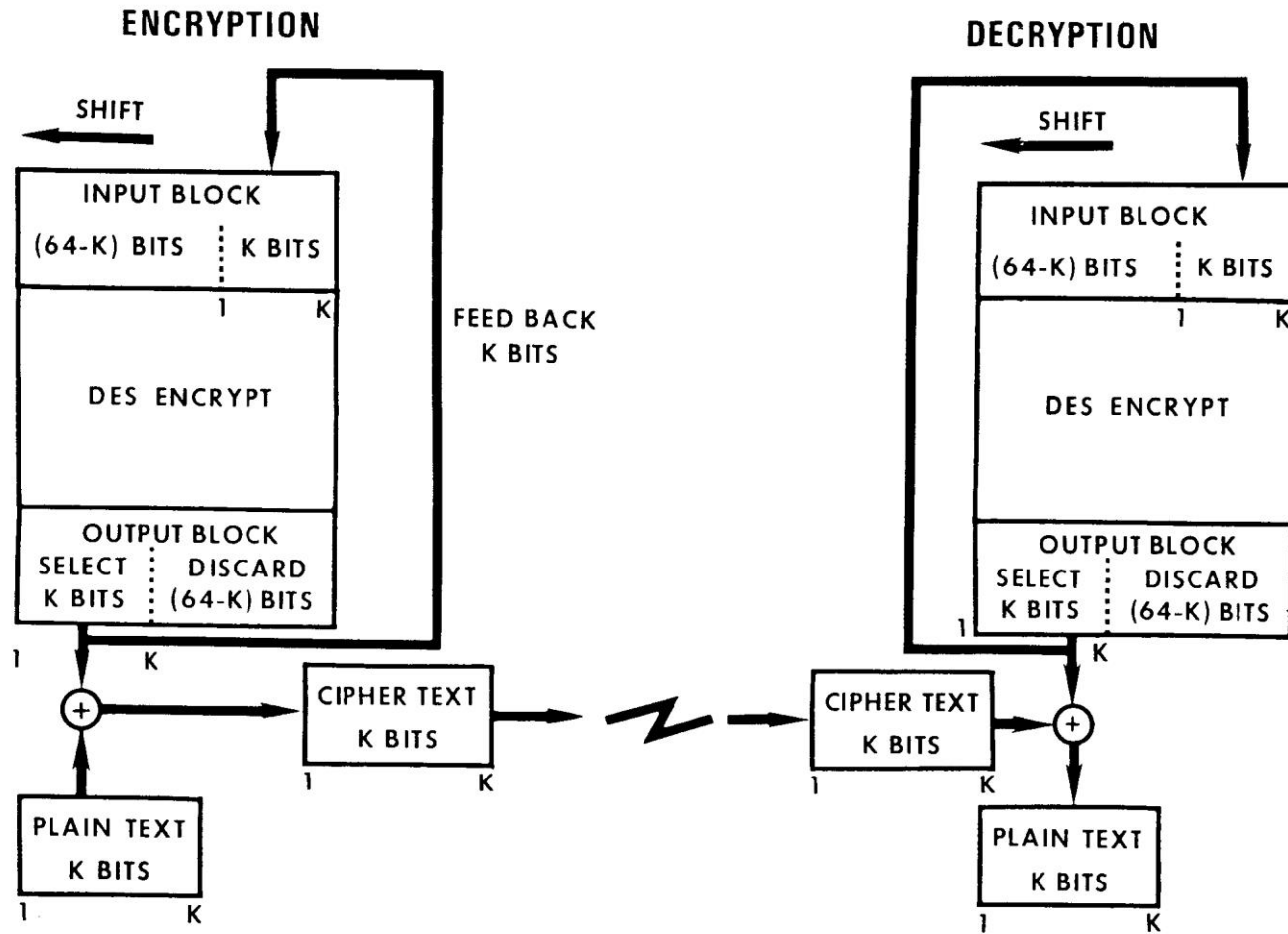


FIGURE 4: K-BIT OUTPUT FEEDBACK (OFB) MODE

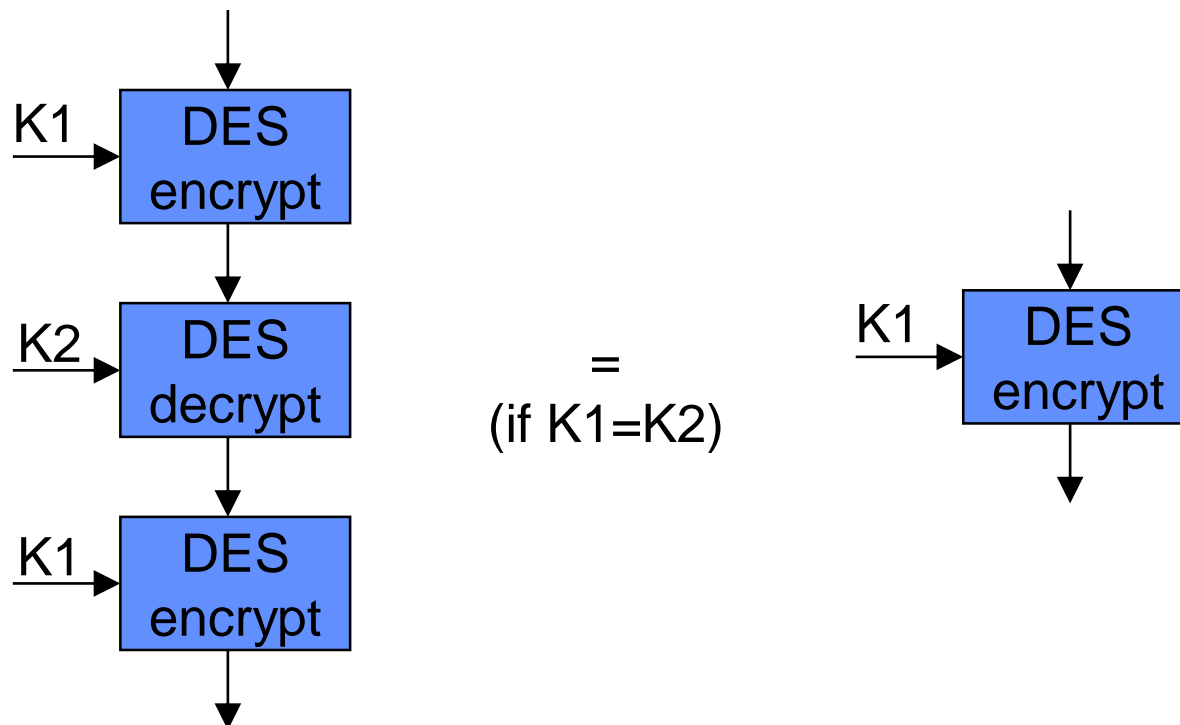


INPUT BLOCK INITIALLY CONTAINS AN INITIALIZATION VECTOR (IV) RIGHT JUSTIFIED.

EDE

3DES, DES-EDE

- Velikost bloku 112 bitů
- Velikost bloku 64 bitů
- ANSI X9.17, ISO 8732 standard
- Double DES není bezpečný
 - CPA útok Merkle-Hellman meet-in-the-middle - 2^{n+1} pokusů



Proudové šifry

Definice

- **Bloková šifra**
 - Data jsou rozdělena na bloky pevné délky a po blocích zašifrována
 - V případě potřeby jsou bloky zarovnány (padding)
- **Proudová šifra**
 - Data jsou šifrována bit po bitu (bajt po bajtu), tak, jak jsou předkládána šifrovacímu mechanismu
- **Většina algoritmů jsou blokové šifry**

Proudová šifra

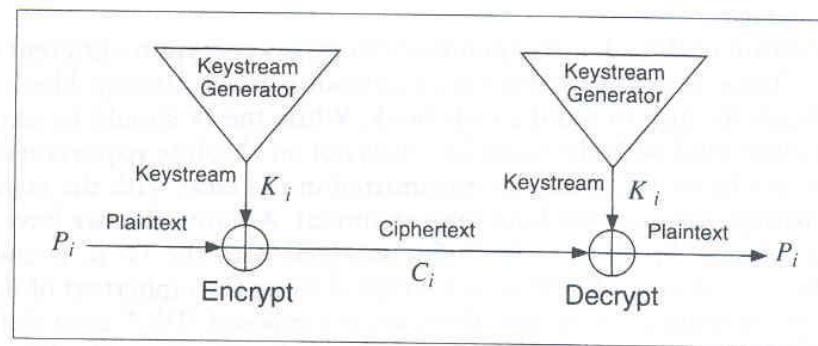
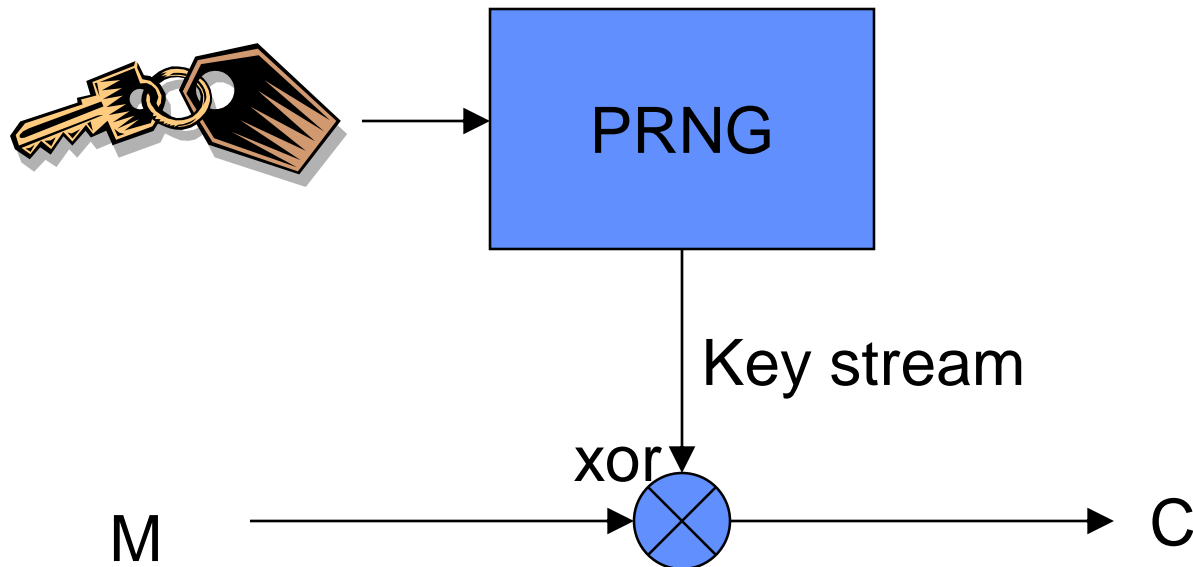


Figure 9.6 Stream cipher.

Synchronnní proudové šifry

- Pseudonáhodná posloupnost (key stream) je nezávislá na zprávě
- Ciphertext is usually XOR of plaintext and key stream
- Např. Vernamova šifra, DES v Output Feedback (OFB) režimu

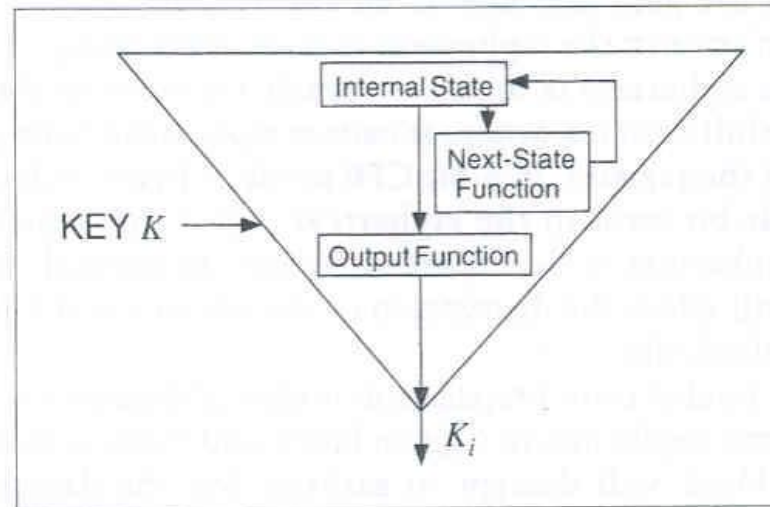


Figure 9.7 Inside a keystream generator.

Samosynchronizující proudové šifry

- Každý bajt pseudonáhodné posloupnosti je závislý na pevném počtu (např. 1) předcházejících bajtů šifrovaného textu
- Umí se resynchronizovat
- Např.: Autokey, DES v Cipher Feedback (CFB) režimu

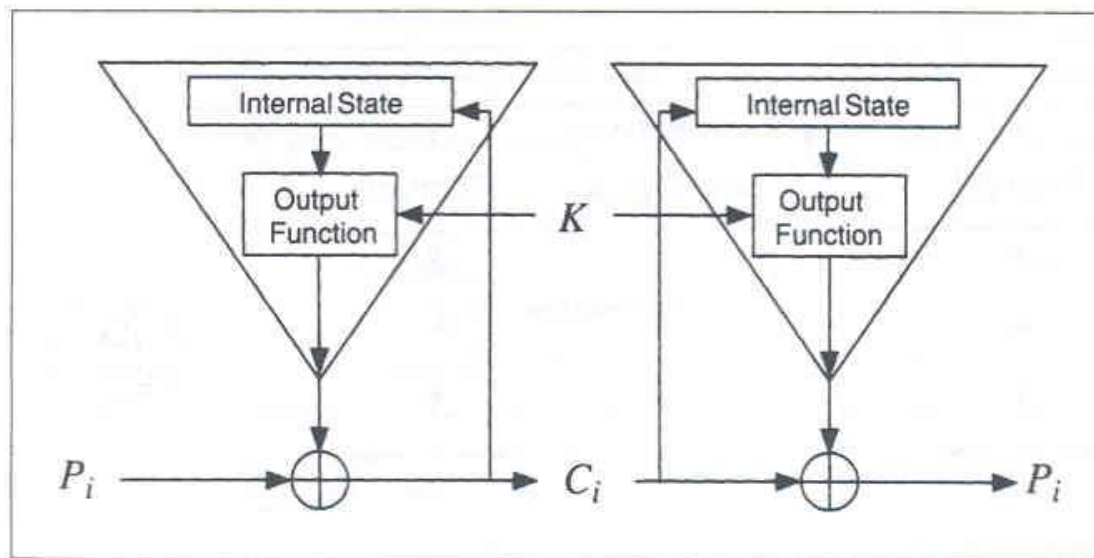


Figure 9.8 A self-synchronizing keystream generator.

Další blokové šifry

International Data Encryption Algorithm (IDEA)

- **Šifruje 64-bitové bloky pomocí 128-bitového klíče**
- **Podobně jako DES:**
 - Pracuje v kolech (rounds)
 - Operace je stejná pro šifrování i dešifrování
- **Od DESu se liší:**
 - Navržena, aby byla efektivní v software
 - Nepoužívá S-boxy a P-boxy

AES: The Next Generation

- **Advanced Encryption Standard (FIPS PUB 197)**
 - Má odstranit nedostatky DES
 - Založený na algoritmu Rijndael algorithm
 - » Joan Daemen and Vincent Rijmen, Belgie
 - U. S. od Nov. 26, 2001, platný od May 26, 2002
 - Délky klíčů 128, 192 a 256 bitů
 - Velikost bloku 128 bitů
 - » Platí pro AES, Rijndael dovoluje i jiné velikosti

Délky klíčů a počet kol

AES-128 – 10 kol

AES-192 – 12 kol

AES-256 – 14 kol



Asymetrická kryptografie

Petr Hanáček
Faculty of Information Technology
Technical University of Brno
Božetěchova 2
612 66 Brno
tel. (05) 4114 1216
e-mail: hanacek@fit.vutbr.cz

Asymetrické algoritmy

- **Knapsack**
 - Knapsack – první algoritmus, Merkle-Hellman, 1976
- **Faktorizace čísel**
 - RSA
 - Diffie-Hellman
- **Diskrétní logaritmus**
 - DSS (DSA)
 - El Gamal
- **Eliptické křivky**
 - Např. ECDSA

Algoritmus RSA

- **Rivest, Shamir, Adelman 1978**
 - Údajně objeven už v GCHQ (Ellis a Cocks) v roce 1973
- **Asymetrický šifrovací algoritmus s veřejným klíčem**
- **Založený na problému faktorizace velkých čísel**
- **Funguje jako bloková šifra, kde blok je celé číslo mezi 0 a n**

RSA – Generování klíčů

- **Klíče**

- n : veřejný modulus
- e : veřejný exponent (typicky 3 nebo $2^{16}+1$)
- d : soukromý exponent
- p, q : činitele (factors) modulu n
 - » $n = p \times q$
- Musí platit vztah
 - » $d \times e \bmod (p-1)(q-1) = 1$

- Veřejný klíč je (n, e) .

- Soukromý klíč je (n, d) .

- Postup

- Vygeneruj prvočísla p a q , $n=pq$
- Spočti $\Phi(n)=(p-1)(q-1)$
- Zvol hodnotu $e < \Phi(n)$ takovou, že $\gcd(\Phi(n), e) = 1$
- Spočti d tak, že $d = e^{-1} \bmod \Phi(n)$

Šifrování / Dešifrování

- Zpráva m (celé číslo)
- Zašifrovaný text c (celé číslo)
- Šifrování veřejným klíčem
 - $c = m^e \bmod n$
- Dešifrování soukromým klíčem
 - $m = c^d \bmod n$
- Použití
 - Utajení

Šifrování / Dešifrování

- Zpráva m (celé číslo)
- Zašifrovaný text s (signature)
- Šifrování veřejným klíčem
 - $s = m^d \bmod n$
- Dešifrování veřejným klíčem
 - $m = s^e \bmod n$
- Použití
 - Elektronický podpis

Příklad RSA

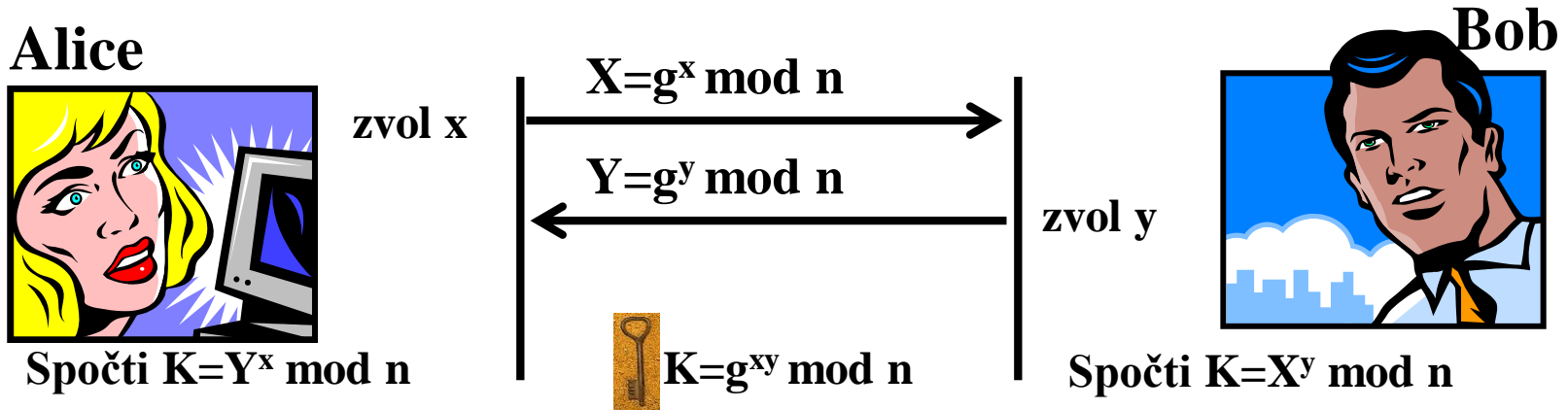
- $p = 11, q = 7, n=77, d = 13, d = 37$
- $m = 15$
- Šifrování
 - $c \equiv m^d \pmod{n}$
 - $c \equiv 15^{37} \pmod{77} = 71$
- Dešifrování
 - $m \equiv c^e \pmod{n}$
 - $m \equiv 71^{13} \pmod{77} = 15$

Útoky na algoritmus RSA

- Pokud útočník umí rozložit n , na činitele p a q , může dopočítat soukromý klíč
- Pokud útočník uhodne hodnotu $(p-1)(q-1)$, vypočte soukromý klíč i bez faktorizace n

Diffie-Hellman

- První algoritmus s veřejným klíčem, založený na problému diskretních logaritmů modulo n
- Protokol:
 - 1. Algoritmus D-H se použije pro ustavení klíče relace K
 - 2. Klíč relace se použije pro šifrování další komunikace
- Zvolení parametrů:
 - Zvolí se velké prvočíslo n , a hodnota g , která nedělí n



Digital Signature Algorithm (DSA)

- Navržen NISTem v r. 1991 jako standard (DSS)
- Založen na diskretních logaritmech
- Má některé nevýhody
 - Nedá se použít pro šifrování nebo distribuci klíčů
 - Rychlejší než RSA při podpisu ale pomalejší při verifikaci
 - Přichází v době, kdy už je značně rozšířeno RSA
 - Obavy, zda neobsahuje zadní vrátka od NIST
- Velikost klíče původně 512 bitů, později zvětšena na 1024 bitů

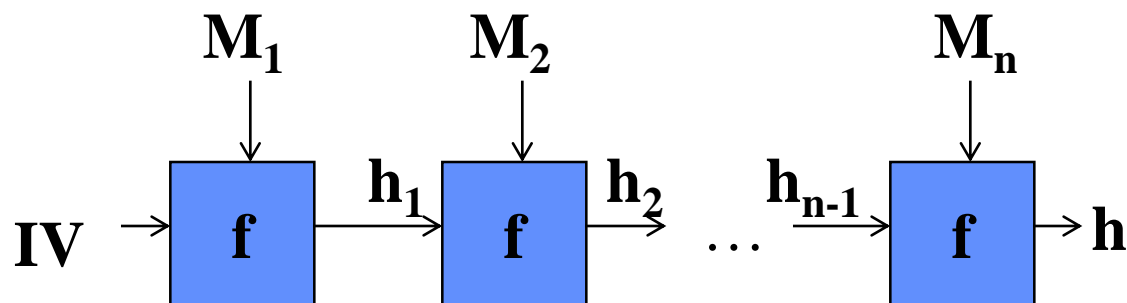
Hašovací funkce

Některé hašovací algoritmy

| | SHA-1 | MD5 (MD4+) | RIPEMD-160 |
|----------------------------------|-----------------------------------|----------------------------|------------------------------------|
| Velikost výstupu | 160 bits | 128 bits | 160 bits |
| Základní velikost bloku | 512 bits | 512 bits | 512 bits |
| Počet kroků | 80 (4 rounds of 20) | 64 (4 rounds of 16) | 160 (5 paired rounds of 16) |
| Maximální velikost zprávy | $2^{64}-1$ bits | unlimited | unlimited |

Konstrukce hašovacích algoritmů

- Jsou obvykle založeny na kompresní funkci f , která pracuje nad bloky M



- Podobné blokovým šifrám v CBC režimu
- Vytvářejí hodnotu haše pro každý blok, která je závislá na hodnotě bloku a hodnotě haše předchozích bloků

Secure Hash Algorithm (SHA)

- SHA byla vytvořena organizací NIST v roce 1993
- Podobná MD5
- Revidována v r. 1995 jako SHA-1
- Revidována v r. 2001 jako SHA-2
 - "SHA-256", "SHA-384", and "SHA-512"

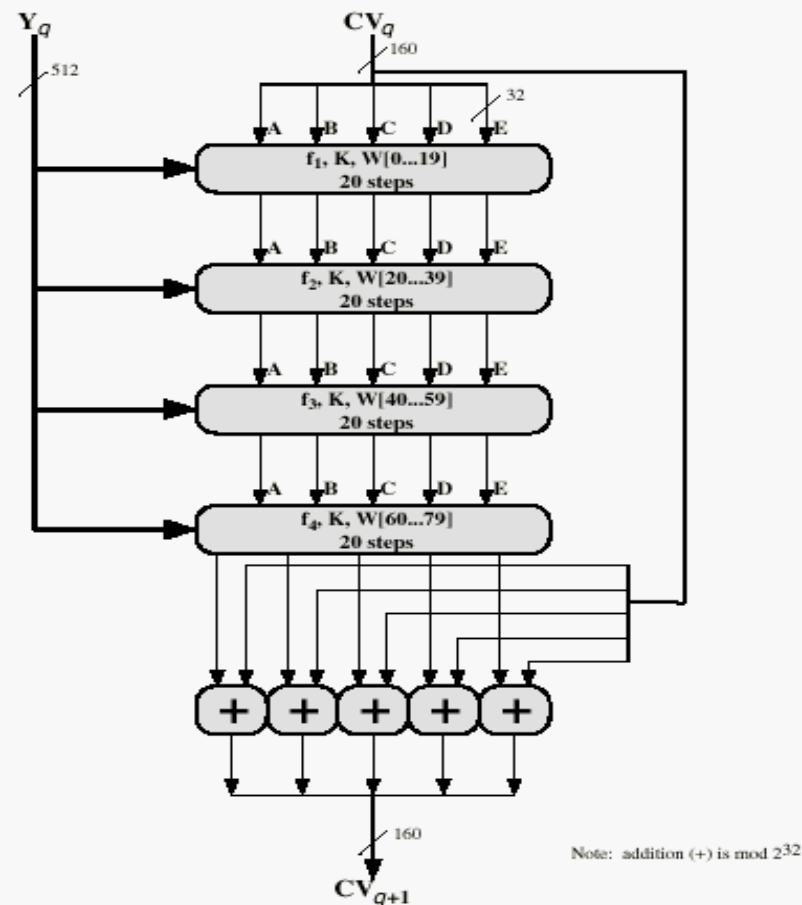


Figure 3.5 SHA-1 Processing of a Single 512-bit Block

MAC

Message Authentication Code

- Message Authentication Code (MAC)

» $MAC = F(Message, Key)$

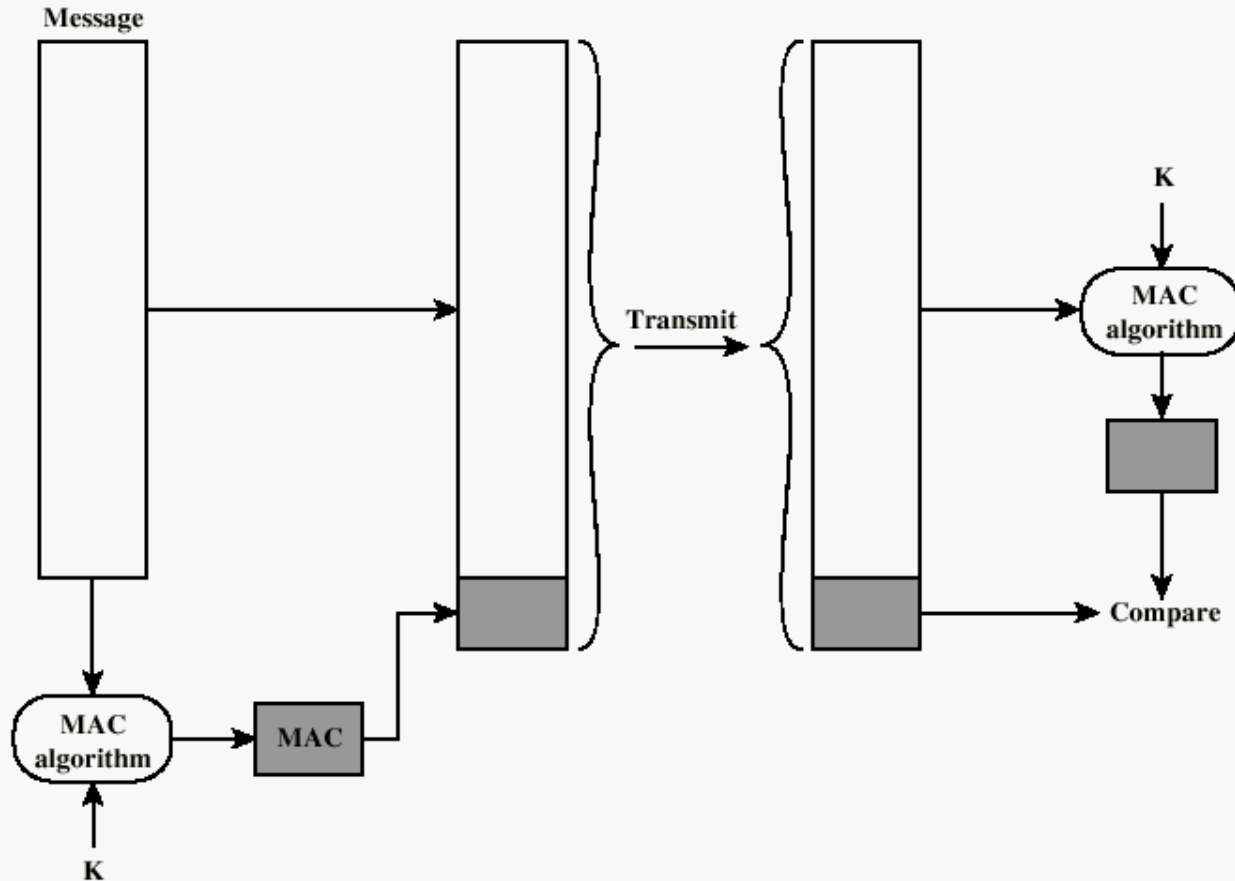
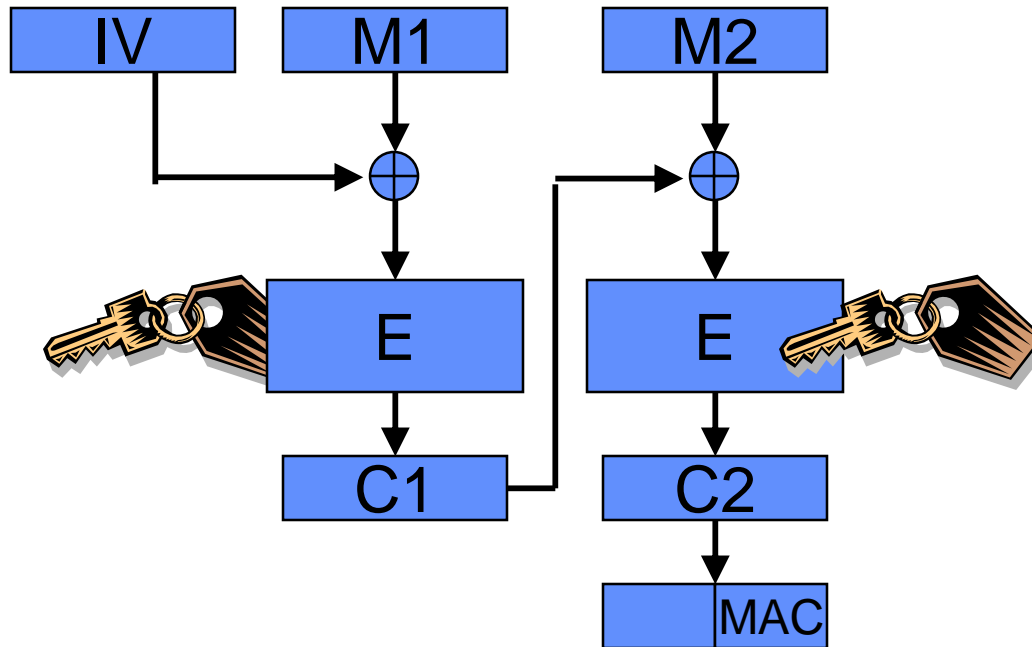


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

CBC MAC



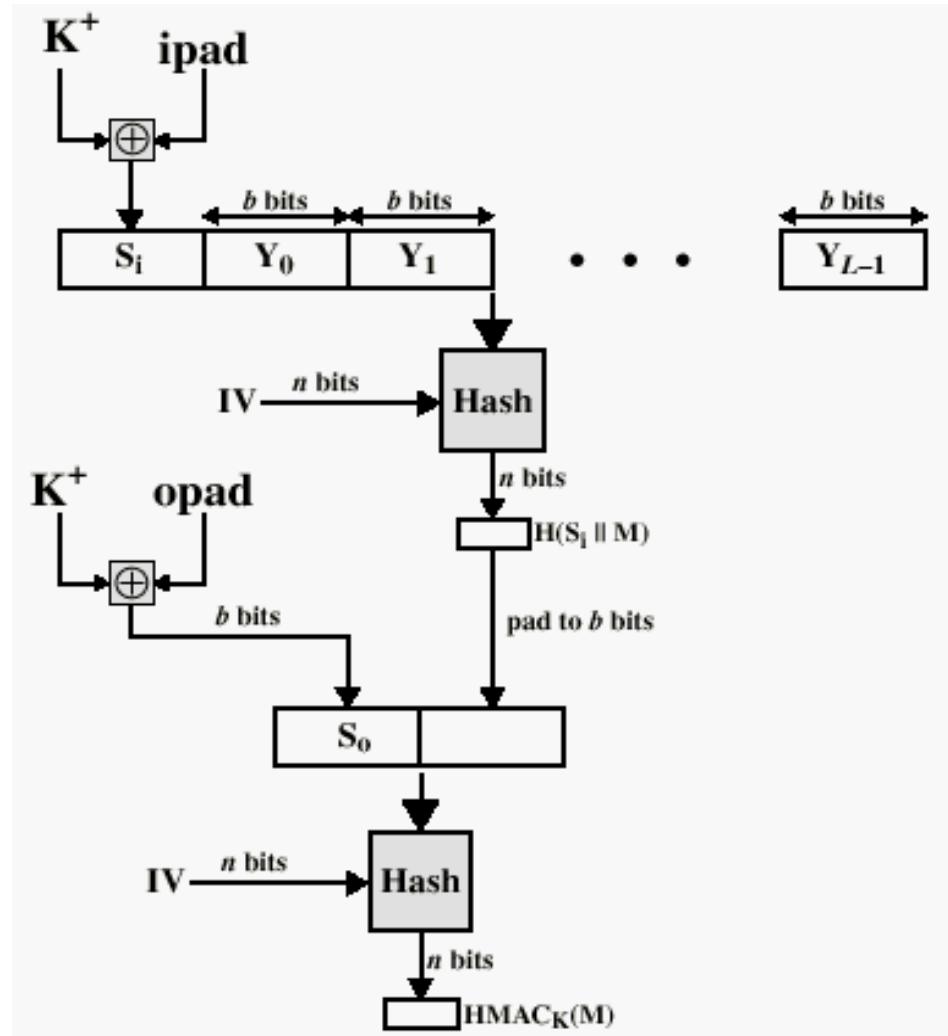
- Typicky 32 bitů z posledního bloku (48, 64)
- Je to dost?

Hash Function MAC (HMAC)

- „Klíčovaný haš“
- **Myšlenka: vytvořit MAC z hašovací funkce**
 - Dodání klíče
 - » „Přihašování klíče“
- **Použití:**
 - IPsec
 - Transport Layer Security (TLS)

HMAC

- Spočte se H1 jako haš konkatence M a K1
- Pro zabránění útoku “dodatečný blok”, se spočte H2 jako haš konkatence H1 a K2
- K1 a K2 používají polovinu bitů klíče K
- Vymaskování bitů:
 - $K^+ = K$ doplněný nulami
 - $ipad = 00110110 \times b/8$
 - $Opad = 01011100 \times b/8$





X.509

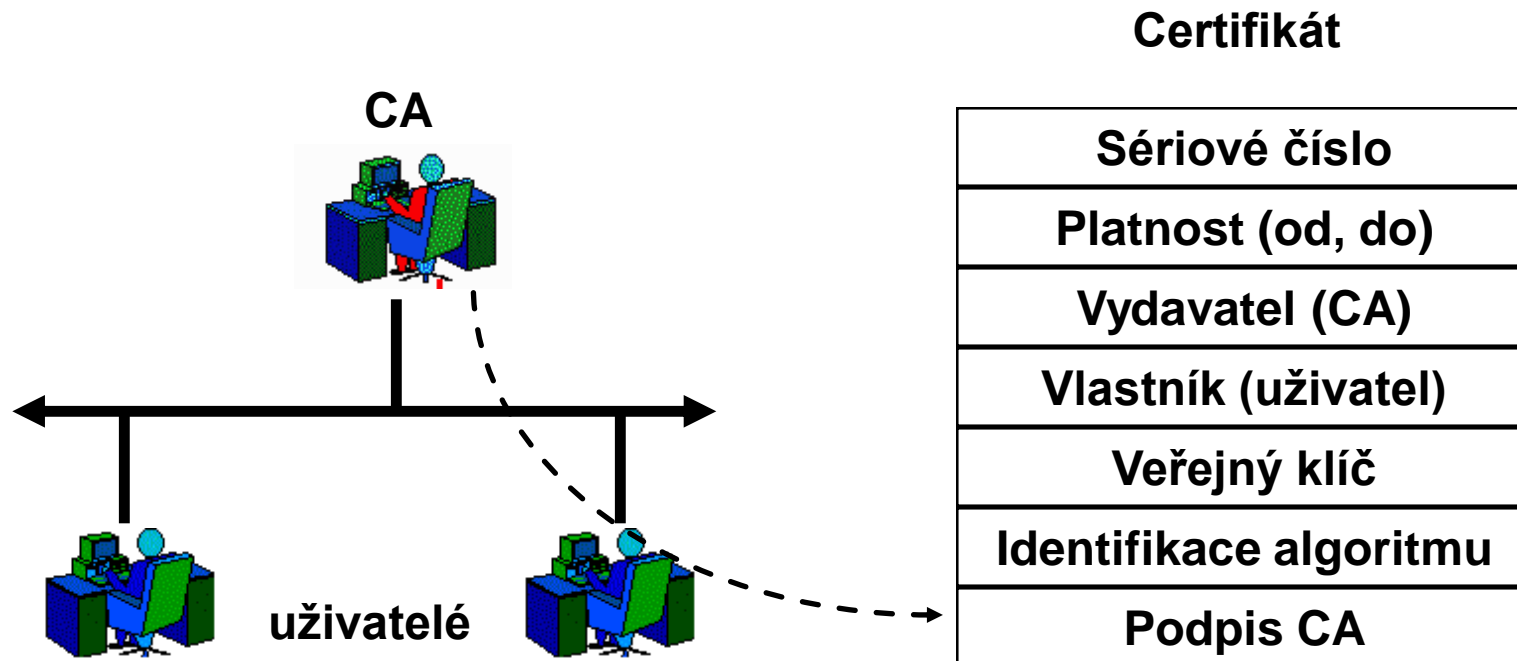
Certifikáty podle X.509

-

Certifikace veřejného klíče

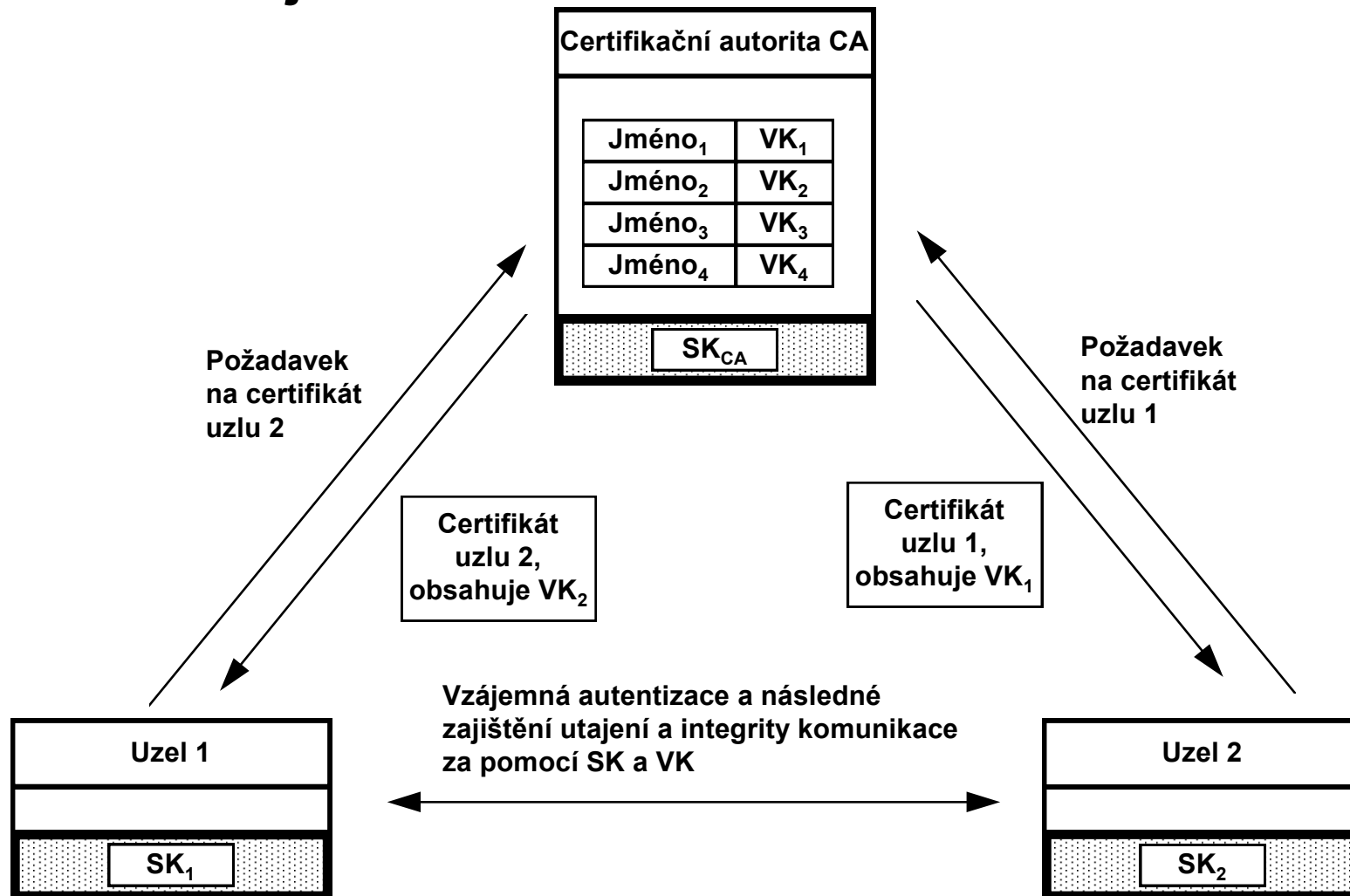
- **otázka autenticity veřejných klíčů (VK)**
 - např. ověřovatel el. podpisu si musí být jist, že VK, který používá k ověřování daného podpisu, je skutečně VK autora zprávy
 - spolehlivá vazba mezi VK a jménem
- **řešení - certifikace VK subjektem, kterému všichni důvěřují**
 - tento prostředník je certifikační autorita (CA)
- **certifikace**
 - CA podepíše VK uživatele a jeho jméno (a další údaje, např. doba platnosti) svým vlastním tajným klíčem
 - tyto údaje, podepsané CA, se nazývají certifikát
 - » certifikát může být ověřen VK certifikační autority
- **ověření VK partnera**
 - ověřením elektronického podpisu certifikátu pomocí VK CA
 - jediný klíč, kterému uživatel musí věřit, je VK CA

Certifikace VK uživatele



Certifikace veřejných klíčů

- Příklad s jedinou CA



Strom CA

- **ve velkých skupinách uživatelů nestačí jediná CA**
- **VK certifikačních autorit mohou být opět certifikovány jinými certifikačními autoritami**
- **stromové struktury certifikačních autorit**
 - křížová certifikace mezi stromy
- **kořenový veřejný klíč**
 - řetěz certifikací nemůže být nekonečný
 - veřejný klíč posledního certifikátu zůstává necertifikovaný - kořenový veřejný klíč
 - autenticita tohoto klíče musí být zajištěna jiným způsobem
 - » získání kurýrem
 - » z papírového média
 - » ...

Výstraha zabezpečení



Informace, které si s tímto serverem vyměníte, nemohou zobrazit ani upravit jiní uživatelé. Nastaly však potíže s certifikátem zabezpečení serveru.



Certifikát zabezpečení vydala společnost, které nedůvěřujete. Prohlédněte si certifikát a rozhodněte se, zda chcete danému certifikačnímu úřadu důvěřovat.



Datum certifikátu zabezpečení je platné.



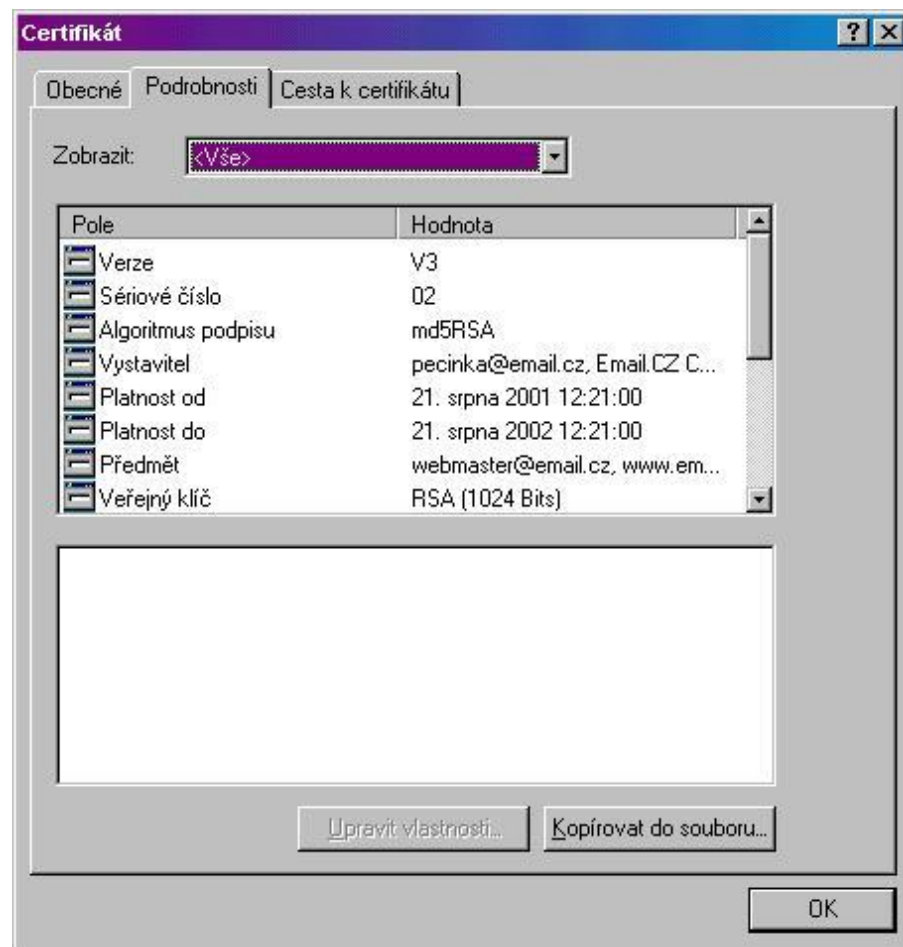
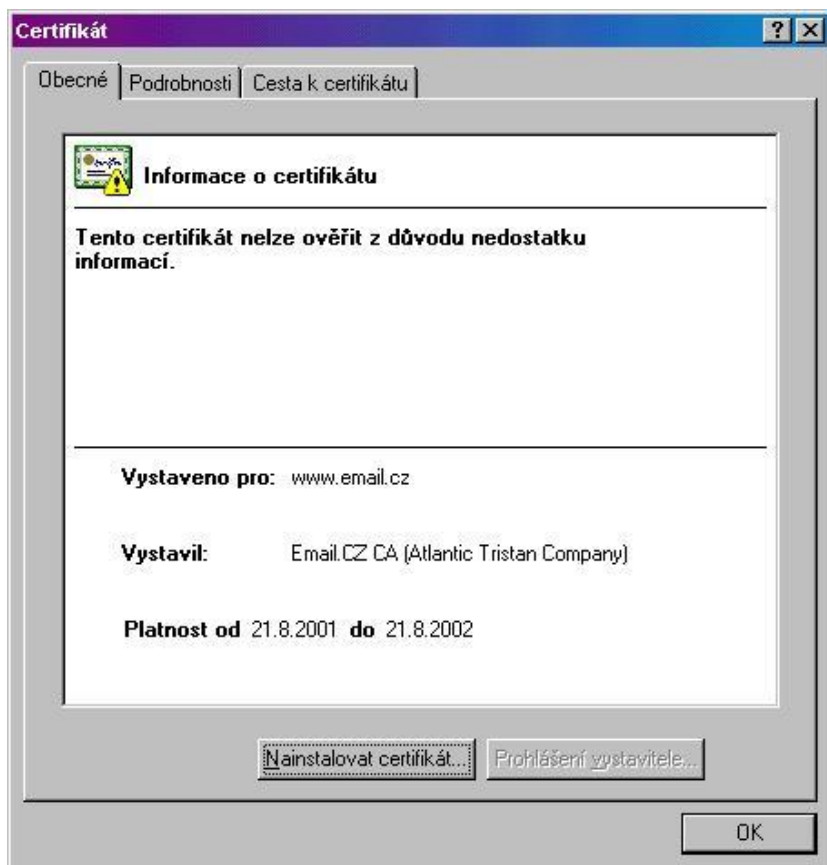
Název na certifikátu zabezpečení souhlasí s názvem stránky, kterou se pokoušíte zobrazit.

Chcete pokračovat?

Ano

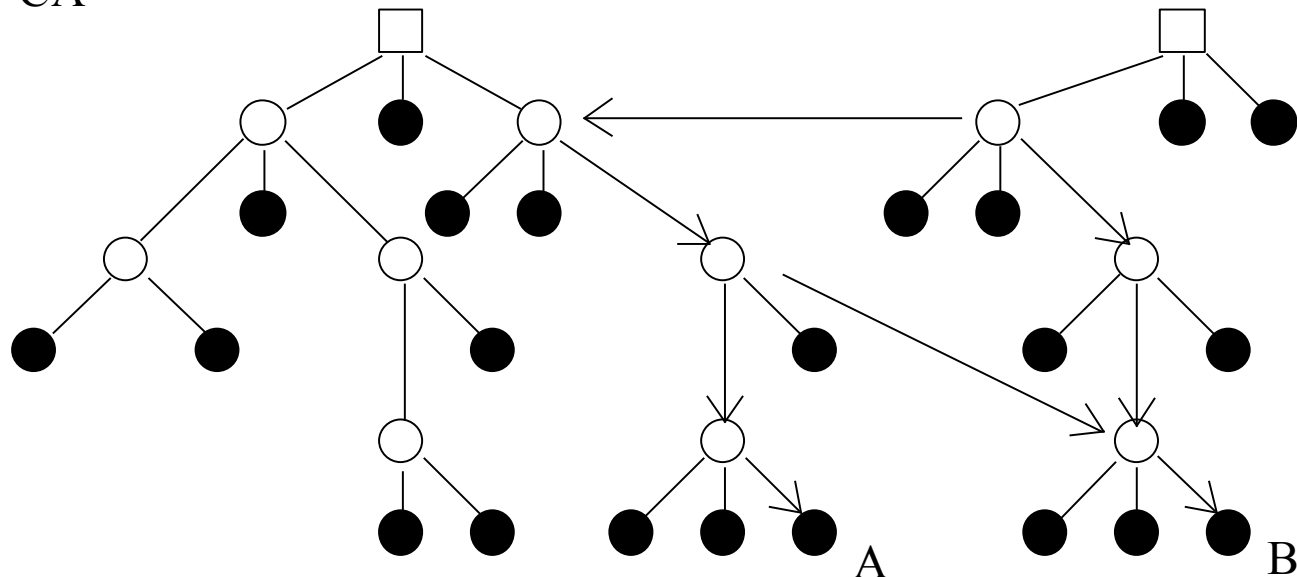
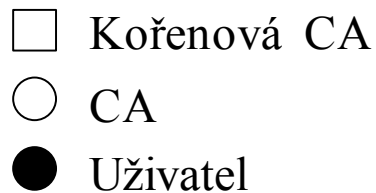
Ne

Zobrazit certifikát



Křížové certifikáty

- Co v případě, že je třeba komunikovat mezi členy různých certifikačních stromů
 - vytvořit společnou kořenovou CA
 - » často není možné
 - křížové certifikáty



Certifikační autorita

- Úkoly CA

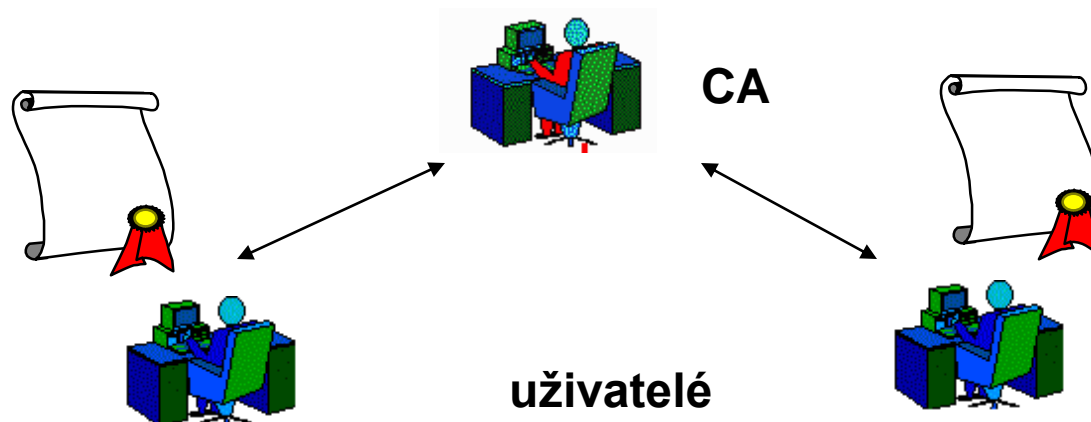
- registrace veřejných klíčů
- distribuce certifikátů
- rušení certifikátů

- Typy CA

- kořenová CA
- “policy” CA - vydává certifikáty CA
- uživatelská CA - vydává certifikáty uživatelům

Certifikát

| |
|------------------------|
| Sériové číslo |
| Platnost (od, do) |
| Vydavatel (CA) |
| Vlastník (uživatel) |
| Veřejný klíč |
| Identifikace algoritmu |
| Podpis CA |



Vydání certifikátu

- uživatel si lokálně vygeneruje klíče
- uživatelské CA zašle prototypový certifikát
- po ověření prototypového certifikátu uživatelská CA pošle uživateli zpět jeho podepsaný certifikát
- **výhody decentralizovaného vytváření klíčů**
 - celý proces je decentralizován a osvobozuje centrální orgán od práce. Uživatelé samotní provádí generování klíčů jen zřídka.
 - soukromé klíče, které jsou vysoce citlivé, nejsou nikdy přenášeny sítí.
 - je zaručeno, že soukromé klíče existují jen v jediném provedení a to v ruce uživatele

Rušení certifikátu


- **Certifikační autorita musí být schopna zrušit vydaný certifikát před skončením doby jeho platnosti.**
- **důvody zrušení certifikátu**
 - byl prozrazen soukromý klíč uživatele
 - změnil se zaměstnavatel uživatele (příslušnost uživatele), čímž je neplatné jméno obsažené v certifikátu
 - uživatel již nemá být certifikován danou CA
 - soukromý klíč CA byl kompromitován
 - uživatel porušil bezpečnostní pravidla CA
- **zrušený certifikát je umístěn na “černou listinu” - seznam zrušených certifikátů - CRL (Certificate Revocation List)**
- **CRL musí být veřejně dostupné, například umístěny v adresáři X.500**

Míra důvěry v certifikáty

- **Třída 1**
 - certifikát zajišťuje pouze jedinečnost jména vlastníka
 - lze jej získat anonymně
- **Třída 2**
 - identita vlastníka musí být ověřena třetí stranou (notářsky ověřený formulář, zaslaný poštou)
- **Třída 3**
 - vlastník musí osobně navštívit CA
 - ověření osobní totožnosti
- **Třída 4**
 - Třída 3 + prokázání oprávněnosti žadatele požadovat certifikát
- **Registrace veřejných klíčů**
 - je třeba pořídit protokol o registraci veřejného klíče, aby uživatel nemohl popřít svůj veřejný klíč

**Registrace
veřejného klíče**

Prohlašuji, že můj veřejný
klíč pro období XX.XX.XX
až XX.XX.XX je následující:


VK

Podpis
uživatele

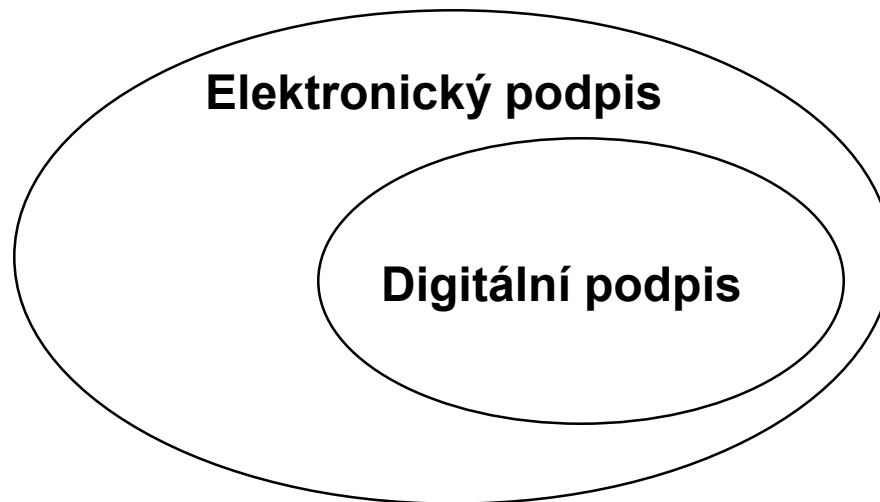
Elektronický podpis



—

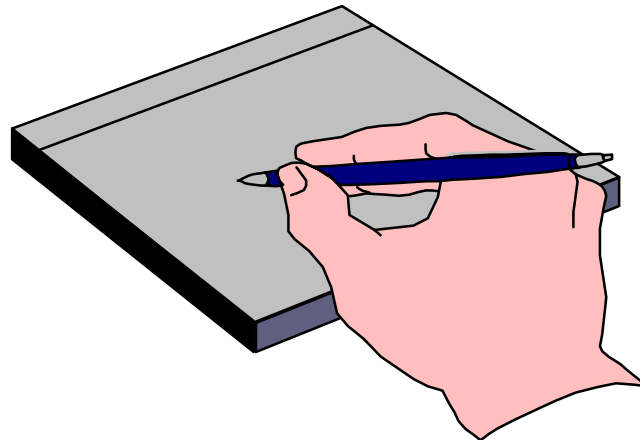
Elektronický vs. digitální

- **Elektronický podpis**
 - vložení textu podpisu do dokumentu
 - vložení naskenovaného obrázku vlastnoručního podpisu do dokumentu
 - ...
 - **Digitální podpis**
 - » založený na použití kryptografických mechanismů
 - v současnosti založený na použití kryptografie veřejným klíčem



Funkce elektronického podpisu

- Zajišťuje autenticitu dokumentu
 - Příjemce dokumentu bezpečně ví, kdo je autorem dokumentu.
- Zajišťuje integritu dokumentu
 - Příjemce dokumentu má jistotu, že obsah dokumentu dokument nebyl během přenosu nebo zpracování modifikován.
- Zajišťuje nepopiratelnost autora dokumentu
 - Autor dokumentu nemůže popřít autorství dokumentu ani jeho obsah.



Porovnání vlastností

| | Manuální podpis | Elektronický podpis |
|---------------------------------------|--|--------------------------------------|
| Autenticita | Ano | Ano |
| Integrita | Nedostatečně | Ano |
| Neodmítnutelnost zodpovědnosti | Ano | Ano |
| Rozlišení originálu od kopie | Ano | Ne |
| Padělatelnost | Ano | Při dodržení postupů Ne |
| Vytvoření | Fyzická přítomnost osoby | Znalost tajemství (soukromého klíče) |
| Ověření | Autentický referenční vzor (+ laboratoř) | Autentický veřejný klíč |

Bezpečnostní služby ISO 7498-2

- **Autentizace**
 - Autentizace spojení
 - Autentizace odesílatele
- **Řízení přístupu**
- **Důvěrnost**
 - Důvěrnost spojení
 - Důvěrnost přenosu zpráv
 - Důvěrnost toku dat
- **Integrita**
 - Integrita spojení s opravou,
 - Integrita spojení bez opravy
 - Integrita přenosu zpráv
- **Nepopiratelnost**
 - Nepopiratelnost odesílatele
 - Nepopiratelnost doručení

KONEC