Bezpečnost v IT – 2. přednáška

Založeno na materiálech dr. Bartla

Radek Janoštík

Univerzita Palackého v Olomouci

22. 2. 2024

Outline

- Aktuální (kyber)bezpečnostní situace
- Kryptografie
  - Terminologie
  - Symetrické šifrování
  - Klasické šifry
  - Frekvenční analýza
- Rest: Sociální inženýrství
- Doporučená četba

Aktuální (kyber)bezpečnostní situace

- Sledujete zprávy z dění v kyberprostoru? Jaké?
- Securence (antispam as a service) uniklo velké množství emailů
- Keytrap chyba v resolverech DNSSEC (nadměrná zátěž CPU)
- Eskalace práv v antiviru ESET – mazání souborů běžným uživatelem
- Něco dalšího?

Kryptografie

Scénář

- odesilatel chce poslat příjemci zprávu
- požaduje však bezpečnost odeslání:

Obsah zprávy je schopen přečíst pouze příjemce a nikdo jiný

Co znamená ”krypto”?

- z řečtiny ”kruprós”– skryté, utajené
- v angličtině ”crypto”asi od roku 1760

Kryptografie

- *kryptografie* . . . věda o utajování zpráv
- kryptografické metody zajišťují:
  - důvěrnost dat – utajení obsahu komunikace (nikoliv komunikace samotné, tím se zabývá steganografie)
  - autentičnost (původnost, hodnověrnost) zprávy – příjemce má možnost zjistit původ zprávy
  - neodmítnutelnost – odesilatel nemůže popřít, že zprávu odeslal
  - integritu zprávy – příjemce má možnost zjistit, jestli během přenosu nedošlo je změně zprávy (úmyslné změně nebo vlivem technické poruchy)

Kryptografie vs. kryptologie

- *kryptoanalýza* . . . věda o luštění šifrovaných zpráv
- *kryptologie* . . . věda zahrnující kryptografii a kryptoanalýzu
- termín kryptografie se však často používá ve významu termínu kryptologie

Kryptografie – terminologie

- *otevřený text* (message, plaintext) – zpráva určená k odeslání
- *šifrování* – proces úpravy otevřeného textu, který ukryje jeho obsah; převede ho do tvaru, který *není srozumitelný*
- *zašifrovaný text, kryptogram* (ciphertext) – výsledek aplikace šifrování na otevřený text
- *dešifrování* – opačný proces k šifrování ion) – matematická funkce provádějící šifrování
- *dešifrovací funkce* (decryption function) – matematická funkce provádějící dešifrování
- *šifra* (cipher) – společné označení pro šifrovací a dešifrovací funkci
- *kanál* (channel) – komunikační spoj, např. Internet, LAN, apod.

Kryptografie

Terminologie:

- Alice – odesilatel (sender)
- Bob – příjemce (receiver)
- Eva (někdy také Oskar) – útočník, protivník (**eave**sdropper, adversary, bad guy)

- *kryptografický modul* – zařízení nebo program zajišťující šifrování, dešifrování, podpisování apod.
  - kryptografický modul zamýšleným způsobem komunikuje se svým okolím prostřednictvím vstupně/výstupních kanálů
  - činností kryptografického modulu vznikají postranní kanály – nežádoucí způsob výměny informací mezi modulem a okolím

Něco málo z historie

- kryptografie je v současnosti spojována s moderními komunikačními technologiemi, je však velmi starým oborem

Např.:

- 2000 let př.n.l., starověký Egypt – tajné hieroglyfy
- starověké Řecko – Řecká skytalé

Něco málo z historie

- 100-44 př.n.l., starověký Řím – Caesarova šifra
- římský historik Gaius Suetonius Tranquillus píše:

  „Existují také Caesarovy dopisy Cicerovi o známých věcech, ve kterých psal tajným písmem, pokud něco muselo být důvěrně sděleno. Změnil pořadí písmen tak, že nešlo zjistit jediné slovo. Pokud někdo chtěl toto rozluštit a poznat obsah, musel dosadit čtvrté písmeno abecedy, tedy D, za A, a podobně toto provést se zbývajícími písmeny."

- Caesarova šifra je jednoduchá monoabecední posouvací šifra
- nemění četnosti výskytu znaků
- jednoduché prolomit hrubou silou

Něco málo z historie

- 15. století, Leon Battista Alberti – italský architekt, historik umění a matematik
- vynalezl polyabecední šifru
- zkonstruoval šifrovací zařízení – *Formula* (používal se téměř 500 let)
- dva kotouče na jedné ose
- vnější kotouč (*Stabilis*) – abeceda otevřeného textu
- vnitřní kotouč (*Mobilis*) – abeceda šifrovaného textu
- pracuje jako jednoduchá posouvací šifra, nebo složitěji jako polyabecední šifra

Něco málo z historie

Něco málo z historie

- 16. století, Blaise de Vigenère – francouzský diplomat, rozvinutí polyabecední šifry
- roku 1586 vyšla jeho knihu *Traicté des Chiffres*, ve které popsal všechny doposud známé šifry
- přelom 19. a 20. století, Arthur Scherbius – německý vynálezce, elektrifikovaná verze Albertiho šifrovacího stroje: Enigma

Enigma

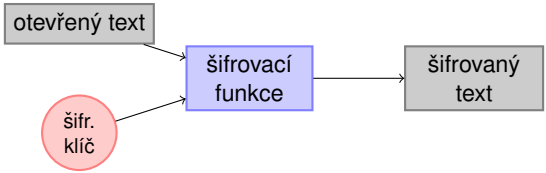
Omezené šifry

- bezpečnost šifrování je založena na utajení způsobu, jakým šifra (šifrovací a dešifrovací funkce) pracuje
- na první pohled dobrý nápad: utajíme šifrovací algoritmus, zvýšíme bezpečnost šifry
- z praktického pohledu nevýhodné
- uvažujeme skupinu uživatelů nějaké omezené šifry, pak
  - může dojít k odhalení principu činnosti šifry
  - odchodem jednoho člena skupiny je nutno šifru změnit
  - nemožnost normalizace – každá skupina si musí vytvořit svoje vlastní hardwarové a softwarové nástroje
  - nemožnost kontroly kvality – pokud ve skupině není skutečně dobrý kryptograf, skupina si nemůže být jistá kvalitou šifry
- dnes se nevyužívají (Enigma) $\Rightarrow$ memorandum:
  „Při posuzování bezpečnosti šifrovacího systému vycházíme z předpokladu, že nepřítel má přístroj k dispozici“

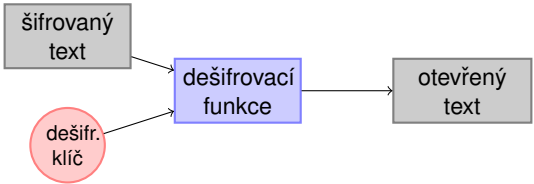
Šifry založené na klíči

- Kerckhoffův princip: bezpečnost šifry závisí pouze na utajení klíče, nikoliv na utajení šifrovací a dešifrovací funkce
- princip šifry může být zveřejněn (a tedy i standardizován)

Šifrovací proces:



Dešifrovací proces:



Šifry založené na klíči

- $\mathcal{M}$ – konečná množina všech zpráv
- $\mathcal{C}$ – konečná množina všech zašifrovaných zpráv
- $\mathcal{K}$ – konečná množina všech klíčů
- $e : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ – šifrovací funkce
- $d : \mathcal{C} \times \mathcal{K} \to \mathcal{M}$ – dešifrovací funkce

Definice (Claude E. Shannon)

Šifra založená na klíči je pětice $\langle \mathcal{M}, \mathcal{C}, \mathcal{K}, e, d \rangle$ taková, že pro libovolný šifrovací klíč $k_e \in \mathcal{K}$ a jemu odpovídající dešifrovací klíč $k_d \in \mathcal{K}$ platí

$$d(e(x, k_e), k_d) = x$$

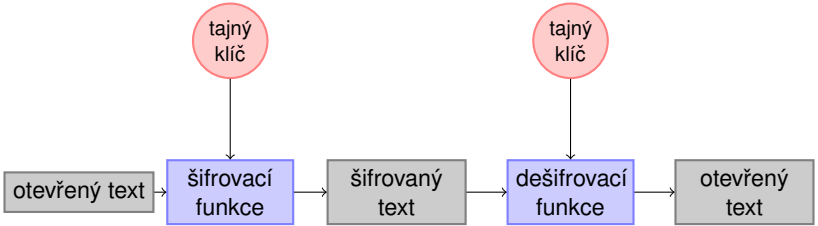
pro všechna $x \in \mathcal{M}$. Krátce budeme mluvit o šifře.

Symetrické šifry

- klíče pro šifrování a dešifrování jsou identické nebo mezi nimi existuje jednoduchý vztah (obousměrný)
- Alice a Bob tedy sdílí stejnou znalost (klíč) a oba umí šifrovat i dešifrovat
- jejich vztah je tedy symetrický, proto *symetrická* šifra
- příklad: všechny klasické šifry (např. posouvací, Vigenèrova), Enigma; z nových šifer např. RC2, DES a jeho varianty (např. Triple DES), AES, Blowfish, IDEA

Symetrické šifry

- postup:
  1. Alice a Bob se domluví na klíči
  2. Alice zašifruje zprávu pomocí klíče
  3. šifrovaná zpráva může být poslána Bobovi přes nezabezpečený komunikační kanál
  4. Bob dešifruje zprávu pomocí klíče
- odesilatel i příjemce musí udržovat klíč v tajnosti → často se také mluví o *šifrování s tajným klíčem* (*private-key cryptography*)



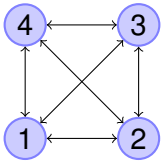
Symetrické šifry

Výhoda:

- šifrování i dešifrování je velmi rychlé

Nevýhody:

- bezpečnost
  - tajný klíč musí být distribuován mezi komunikujícími uživateli
  - nebezpečí odhalení tajného klíče třetí stranou
- velký počet klíčů, složitý key management
  - počet klíčů = počet všech komunikačních kanálů
  - jak rychle roste počet klíčů v závislosti na počtu uživatelů?



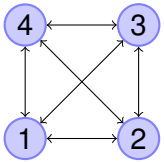
Symetrické šifry

Výhoda:

- šifrování i dešifrování je velmi rychlé

Nevýhody:

- bezpečnost
  - tajný klíč musí být distribuován mezi komunikujícími uživateli
  - nebezpečí odhalení tajného klíče třetí stranou
- velký počet klíčů, složitý key management
  - počet klíčů = počet všech komunikačních kanálů
  - počet klíčů roste kvadraticky, n uživatelů potřebuje $\frac{n \cdot (n-1)}{2}$ klíčů



- problémy řeší asymetrické šifrování

Jak vypadají šifrovací a dešifrovací funkce?

- otevřenou zprávu zakódujeme do posloupnosti čísel, např. s využitím ASCII
- šifrovací a dešifrovací funkce budou využívat aritmetické operace: sčítání, odčítání, násobení, atd.
- jak tyto operace definovat na konečných číselných množinách?
- využijeme modulární aritmetiku

Modulární aritmetika – opakování pojmů

Prvočísla, (ne)soudělnost, největší společný dělitel:

- prvočíslo
- jednoznačný rozklad kladného celého čísla na prvočísla, např. $60 = 2^2 \cdot 3^1 \cdot 5^1$
- největší společný dělitel $\gcd(a, b)$ čísel a a b – Euklidův algoritmus
- $a, b \in \mathbb{Z}$ jsou nesoudělná čísla, jestliže $\gcd(a, b) = 1$
- pro každé $a \in \mathbb{Z}$, $n \in \mathbb{N}$ existují $k \in \mathbb{Z}$ (dělitel) a $r \in \{0, \ldots, n-1\}$ (zbytek) tak, že $a = k \cdot n + r$
- jestliže je zbytek nulový, pak říkáme, že n dělí a; píšeme $n|a$
- platí: jestliže $\gcd(a, b) = 1$ a $a|bc$, pak $a|c$ (využijeme v afinní šifře)

Modulární aritmetika

Vlastnosti největšího společného dělitele

Dodefinujeme: $\gcd(0, 0) = 0$

Pro každé $k \in \mathbb{N}$ platí:

$$\gcd(a, b) = \gcd(b, a)$$
$$\gcd(a, b) = \gcd(-a, b)$$
$$\gcd(a, 0) = |a|$$
$$\gcd(a, b) = \gcd(a - k \cdot b, b)$$

Modulární aritmetika

Výpočet největšího společného dělitele

$$
\begin{aligned}
a &= b \cdot k_0 + r_0 \\
b &= r_0 \cdot k_1 + r_1 \\
r_0 &= r_1 \cdot k_2 + r_2 \\
r_1 &= r_2 \cdot k_3 + r_3 \\
&\vdots
\end{aligned}
$$

- skončí tento výpočet?

Modulární aritmetika

Výpočet největšího společného dělitele

$$
\begin{aligned}
a &= b \cdot k_0 + r_0 \\
b &= r_0 \cdot k_1 + r_1 \\
r_0 &= r_1 \cdot k_2 + r_2 \\
r_1 &= r_2 \cdot k_3 + r_3 \\
&\vdots \\
r_{n-2} &= r_{n-1} \cdot k_n + r_n \\
r_{n-1} &= r_n \cdot k_{n+1}
\end{aligned}
$$

- ano, skončí
- platí totiž: $b > r_0 > r_1 > r_2 > \ldots$
- množina $\mathbb{N}$ je *dobře uspořádaná*: existuje konečné číslo n takové, že $r_{n+1} = 0$ (tzn. $r_n | r_{n-1}$)

Modulární aritmetika

Výpočet největšího společného dělitele

$$
\begin{aligned}
a &= b \cdot k_0 + r_0 \\
b &= r_0 \cdot k_1 + r_1 \\
r_0 &= r_1 \cdot k_2 + r_2 \\
r_1 &= r_2 \cdot k_3 + r_3 \\
&\vdots \\
r_{n-2} &= r_{n-1} \cdot k_n + r_n \\
r_{n-1} &= r_n \cdot k_{n+1}
\end{aligned}
$$

- opakovaným použitím vlastnosti $\gcd(a, b) = \gcd(a - k \cdot b, b)$ dokážeme, že

$$\gcd(a, b) = r_n$$

- pozn.: není potřeba předpokládat $a \geq b$; pokud $a < b$, první řádek vymění a a b

Modulární aritmetika

Kongruence podle modulu:

- $a, b \in \mathbb{Z}$ jsou kongruentní podle modulu $n \in \mathbb{N}$, jestliže a a b dávají stejný zbytek po dělení číslem n; píšeme $a \equiv b \pmod{n}$
- např.: $27 \equiv 15 \pmod{6}$, protože $27 = 4 \cdot 6 + 3$ a $15 = 2 \cdot 6 + 3$
- platí: $a \equiv b \pmod{n}$ právě tehdy, když $n|(a - b)$
- např.: $11 \equiv 5 \pmod{3}$, protože $3|(11 - 5)$
- relace $\equiv$ je ekvivalence; $\equiv$ pro daný modul n indukuje rozklad na $\mathbb{Z}$
- třídy tohoto rozkladu se nazývají zbytkové třídy podle modulu n
- zbytková třída podle modulu n určená prvkem a:

$$\begin{aligned}[a]_n &= \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} \\ &= \{k \cdot n + a \mid k \in \mathbb{Z}\}\end{aligned}$$

- např.: $[5]_3 = \{\ldots, -1, 2, 5, 8, 11, \ldots\}$
- např.: množina sudých a lichých čísel

Modulární aritmetika

Množina zbytkových tříd:

- množina zbytkových tříd:
$$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}$$
- zřejmě platí: $[a]_n = [b]_n$ právě tehdy, když $a \equiv b \pmod{n}$
- např.: $[5]_3 = [11]_3$, protože $5 \equiv 11 \pmod{3}$
- zejména platí, že:
$$[a]_n = [r]_n,$$
kde r je zbytek po dělení čísla a číslem n
- např.: $[5]_3 = [11]_3 = [2]_3$
- celkem tedy můžeme psát:
$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$$
- zkrácený zápis:
$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

Modulární aritmetika

Operace na množině zbytkových tříd:

- na $\mathbb{Z}_n$ definujeme operace sčítání $+$ a násobení $\cdot$ následovně:

$$[a]_n + [b]_n = [a + b]_n$$
$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

- pozn.: relace $\equiv$ modulo n je kompatibilní s $+$ a $\cdot$
- např.: uvažujeme $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- píšeme: $(1 + 2) \bmod 4 = 3$, $(3 + 3) \bmod 4 = 2$

Modulární aritmetika

Operace na množině zbytkových tříd:

- např. uvažujeme $\mathbb{Z}_2 = \{0, 1\}$
- strojové instrukce:
  - XOR (výše uvedené $+$) – logická operace exkluzivní disjunkce
  - AND (výše uvedené $\cdot$) – logická operace konjunkce
- Používá se u bitově orientovaných šifer, např. LSFR, Feistelova šifra používaná v DES atd.

Modulární aritmetika – trochu algebry

Inverzní prvky v $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n, \cdot)$:

- $(\mathbb{Z}_n, +)$ je komutativní grupa ... existuje v ní neutrální prvek $[0]_n$ a ke každému prvku $[a]_n$ prvek inverzní $[-a]_n$
- pozn.: $(\mathbb{Z}_n, +)$ je cyklická grupa (generovaná prvkem $[1]_n$)
- $(\mathbb{Z}_n, \cdot)$ je pouze komutativní monoid ... existuje zde sice neutrální prvek $[1]_n$, ale obecně nemusí existovat ke každému prvku prvek inverzní
- např.: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, inverzní prvek k 1 je 1 ($(1 \cdot 1) \bmod 4 = 1$), inverzní prvek ke 3 je 3 ($(3 \cdot 3) \bmod 4 = 1$), prvek 2 ale inverzi nemá
- jaké prvky nemají inverzi v $\mathbb{Z}_9 = \{0, \ldots, 8\}$
- dál platí, že $(\mathbb{Z}_n, +, \cdot)$ je okruh (s komutativní operací $\cdot$)

Modulární aritmetika

Inverzní prvky v $(\mathbb{Z}_n, \cdot)$:

- platí: prvek a má inverzi v $(\mathbb{Z}_n, \cdot)$ právě tehdy, když $\gcd(a, n) = 1$

Eulerova funkce:

- Eulerova funkce φ: $\varphi(n)$ je počet přirozených čísel menších než n a nesoudělných s n
- vlastnosti Eulerovy funkce:

(i) $\varphi(p) = p - 1$ pro libovolné prvočíslo p

(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ pro libovolná nesoudělná čísla a, b

(iii) jestliže $a = \prod_{i=1}^{m} p_i^{e_i}$ je rozklad čísla a na prvočísla p_i, pak

$$\varphi(a) = \prod_{i=1}^{m} (p_i^{e_i} - p_i^{e_i - 1})$$

- např.: $60 = 2^2 \cdot 3^1 \cdot 5^1$, takže $\varphi(60) = (4 - 2) \cdot (3 - 1) \cdot (5 - 1) = 16$

Klasické šifry

- symetrické šifry
- budeme používat anglickou abecedu s 26 písmeny
- písmena abecedy jsou kódovány: $\mathtt{A} \to 0$, $\mathtt{B} \to 1$, $\ldots$, $\mathtt{Z} \to 25$
- počítáme tedy v $\mathbb{Z}_{26}$
- všechny šifry se ovšem dají zobecnit na abecedy s n symboly ($\mathbb{Z}_n$)
- dva typy klasických šifer:
  - monoabecední (posouvací, afinní, substituční šifra) – prvky množin $\mathcal{M}$ a $\mathcal{C}$ jsou jednotlivé symboly abecedy, tzn. symbol abecedy je vždy mapován šifrovací funkcí na jediný symbol
  - polyabecední (Viegenèrova šifra) – prvky množin $\mathcal{M}$ a $\mathcal{C}$ jsou posloupnosti symbolů abecedy určité délky, tzn. symbol abecedy je mapován na jeden z několika symbolů
- jiné dělení (podle způsobu šifrování):
  - blokové šifry
  - proudové šifry

Posouvací šifra

- monoabecední šifra; písmeno abecedy je mapováno na jiné písmeno téže abecedy, které je posunuté o určitý počet pozic (tento počet je daný klíčem)

Definice

Nechť $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. Pro $k \in \mathcal{K}$ definujeme šifrovací funkci

$$e(x, k) = x + k$$

a dešifrovací funkci

$$d(y, k) = y - k.$$

- pro $k = 3$ mluvíme o tzv. Caesarově šifře
- kryptoanalýza je založená na *exhaustive key search* (hrubá síla)
- existuje pouze 26 různých klíčů, šifra není bezpečná
- v průměru je správný klíč odhalen po $\frac{26}{2} = 13$ pokusech

Afinní šifra

- monoabecední šifra; písmeno abecedy je mapováno na jiné písmeno téže abecedy pomocí šifrovací funkce:

$$e(x, k) = ax + b,$$

  kde $k = \langle a, b \rangle$
- je nutné ověřit, že je tato funkce injektivní
- např. $e(x, \langle 4, 7 \rangle) = 4x + 7$ není injektivní; x a $x + 13$ se zobrazí na stejné číslo pro libovolné $x \in \mathbb{Z}_{26}$

Afinní šifra

Definice

Nechť $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}$, $\mathcal{K} = \{\langle a, b\rangle \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} \mid \gcd(a, 26) = 1\}$. Pro $k = \langle a, b\rangle \in \mathcal{K}$ definujeme šifrovací funkci

$$e(x, k) = ax + b,$$

a dešifrovací funkci

$$d(y, k) = a^{-1}(y - b).$$

- proč $d(y, k) = a^{-1}(y - b) \bmod \mathbb{Z}_{26}$?
- posouvací šifra je speciálním případem afinní šifry ($a = 1, k = b$)

Afinní šifra

Počet různých klíčů afinní šifry:

- klíč $k \in \mathcal{K}$ je dvojice $\langle a, b \rangle \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$
- a musí být nesoudělné s 26, b se může volit libovolně
- proto existuje $26 \cdot \varphi(26) = 26 \cdot 12 = 312$ různých klíčů
- stále velmi málo klíčů, pro kryptoanalýzu můžeme použít hrubou sílu

Substituční šifra

- monoabecední šifra; písmeno abecedy je mapováno na jiné písmeno téže abecedy podle zvolené permutace této abecedy
- opakování: permutace π množiny X je bijekce na X, tzn. zobrazení $\pi : X \to X$, které je injektivní a surjektivní

Definice

Nechť $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}$, $\mathcal{K} = \{\pi \mid \pi \text{ je permutace } \mathbb{Z}_{26}\}$. Pro $\pi \in \mathcal{K}$ definujeme šifrovací funkci

$$e(x, \pi) = \pi(x),$$

a dešifrovací funkci

$$d(y, \pi) = \pi^{-1}(y).$$

- posouvací a afinní šifra jsou speciálním případem substituční šifry

Substituční šifra

- existuje asi $4 \cdot 10^{26}$ různých klíčů – nemůžeme použít hrubou sílu
- proč $4 \cdot 10^{26}$ klíčů?
- pro srovnání: počet atomů ve vesmíru se odhaduje na 10^{78} až 10^{82}
- přesto to není bezpečná šifra
- kryptoanalýza se provádí s využitím jiných metod (uvidíme později)

Vigenèrova šifra

- polyabecední šifra:
  - prvky $\mathcal{M}$ jsou m-tice písmen abecedy
  - klíčem je také m-tice písmen abecedy; mluvíme o klíčovém slově (keyword)
  - písmeno abecedy může být mapováno na jedno z m písmen téže abecedy (pokud předpokládáme, že je klíč složen z m různých písmen)

Definice

Nechť $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$, $m \in \mathbb{N}$. Pro klíč $\mathbf{k} = \langle k_1, \ldots, k_m \rangle \in \mathcal{K}$ definujeme šifrovací funkci

$$e(\mathbf{x}, \mathbf{k}) = \langle x_1 + k_1, \ldots, x_m + k_m \rangle,$$

a dešifrovací funkci

$$d(\mathbf{y}, \mathbf{k}) = \langle y_1 - k_1, \ldots, y_m - k_m \rangle$$

pro všechna $\mathbf{x} = \langle x_1, \ldots, x_m \rangle \in \mathcal{M}$, $\mathbf{y} = \langle y_1, \ldots, y_m \rangle \in \mathcal{C}$.

Vigenèrova šifra

- existuje 26^m různých klíčů délky m
- není to však bezpečná šifra
- kryptoanalýza se provádí pomocí Kasiského a Friedmannova testu
  - nechám na samostudium, nebude vyžadováno

Kryptoanalýza klasických šifer

Předpoklad:

- Oskar ví, jak funguje šifra, kterou se snaží prolomit (Kerckhoffův princip)
- v opačném případě by byla kryptoanalýza složitější
- použití omezených šifer (princip šifry je utajen) jsme však zavrhli

Typy útoků:

- kryptoanalýza se liší v závislosti na typu informace, kterou má Oskar k dispozici
- mluvíme pak o následujících útocích:
  1. ciphertext only attack
  2. known plaintext attack
  3. chosen plaintext attack
  4. chosen ciphertext attack

Kryptoanalýza klasických šifer

Typy útoků:

1. ciphertext only attack
   - Oskar zná zašifrovanou zprávu
2. known plaintext attack
   - Oskar zná původní zprávu a jí odpovídající zašifrovanou zprávu
3. chosen plaintext attack
   - Oskar získal dočasný přístup ke kryptografickému modulu, který realizuje šifrování; může si vybrat libovolnou zprávu a tu pak zašifrovat
4. chosen ciphertext attack
   - Oskar získal dočasný přístup ke kryptografickému modulu, který realizuje dešifrování; může si vybrat libovolný kryptogram a ten pak dešifrovat

- ve všech případech je snahou Oskara získat klíč

Kryptoanalýza klasických šifer

- kryptoanalýza je často založena na statistických vlastnostech daného jazyka
- Jelikož se nám znak zašifruje vždy na stejný znak $\Rightarrow$ statistické vlastnosti otevřeného textu a kryptogramu by měly být stejné
- uvažujme anglický jazyk s 26 znaky, neuvažujeme mezery
  - Mezery by kryptoanalýzu hodně zjednodušily
  - Spolupráce se slovníkem
- **Frekvenční analýza** založena na (přirozeném) rozdílném výskytu znaků v jazyce
- pro texty psané v anglickém jazyce bylo zjištěno (Beker a Piper):
  - písmeno E se vyskytuje s pravděpodobností asi 0,12
  - písmena T, A, O, I, N, S, H, R mezi 0,06 a 0,08
  - písmena D, L asi 0,04
  - C, U, M, W, F, G, Y, P, B mezi 0,015 a 0,028
  - V, K, J, X, Q, Z asi 0,01

Frekvenční analýza

- Pro angličtinu byly (experimentálně) zjištěny frekvence výskytu písmen:

e	12.702%	m	2.406%
t	9.056%	w	2.360%
a	8.167%	f	2.228%
o	7.507%	g	2.015%
i	6.966%	y	1.974%
n	6.749%	p	1.929%
s	6.327%	b	1.492%
h	6.094%	v	0.978%
r	5.987%	k	0.772%
d	4.253%	j	0.153%
l	4.025%	x	0.150%
c	2.782%	q	0.095%
u	2.758%	z	0.074%

- Na podobném principu je založena i Morseova abeceda

Frekvenční analýza – vylepšení

- Existuje určitá závislost ve výskytu písmen na základě předchozího písmena
- Například písmeno **Q** je téměř vždy následování písmenem **U**
  - `https://en.wikipedia.org/wiki/List_of_English_words_containing_Q_not_followed_by_U`
- Výskyty digramů a trigramů (zdroj: Wiki):

th 1.52	en 0.55	ng 0.18	the 1.81%	for 0.34%	
he 1.28	ed 0.53	of 0.16	and 0.73%	tha 0.33%	
in 0.94	to 0.52	al 0.09	ing 0.72%	tio 0.31%	
er 0.94	it 0.50	de 0.09	ent 0.42%	oft 0.22%	
an 0.82	ou 0.50	se 0.08	ion 0.42%	sth 0.21%	
re 0.68	ea 0.47	le 0.08			
nd 0.63	hi 0.46	sa 0.06			
at 0.59	is 0.46	si 0.05			
on 0.57	or 0.43	ar 0.04			
nt 0.56	ti 0.34	ve 0.04			
ha 0.56	as 0.33	ra 0.04			
es 0.56	te 0.27	ld 0.02			
st 0.55	et 0.19	ur 0.02			

Kryptoanalýza substituční šifry pomocí frekvenční analýzy

- Oskar najde v kryptogramu znak s největší četností, ten je pravděpodobně zašifrovaným písmenem E
- Na základě frekvencí znaků interaktivně hádá možnosti a dívá se, zda částečně rozšifrovaný kryptogram dává smysl
- podobně pokračuje pro další znaky případně digramy a trigramy
  - Případný backtracking
- Možná (polo)automatická spolupráce se slovníkem

Sociální inženýrství

- „Social engineering bypasses all technologies, including firewalls“, Kevin Mitnick
- $\Rightarrow$ Útok na nejslabší článek systémů (jaký?) lidský faktor
- $=$ Využití psychologických triků a forem manipulace k přesvědčení uživatelů k
  - vyzrazení důvěrných informací (a jejich využití později)
  - udělení přístupu (fyzicky, oprávnění, . . .)
  - vyplacení peněz
  - . . .
- Využití částečné znalosti zabezpečení systému k přesvědčení
  - Podvodné emaily, telefonáty: „Ahoj tady Karel z oddělení cyber security, ještě se k mě nedostalo nové heslo, minulý měsíc bylo *StudujUp2022*, prosím tě, jaké je to nové?“
  - Útok na naléhavost, „převleky“, falešné vizitky, moderní plášť neviditelnosti, . . .
- Vše až překvapivě účinné

Sociální inženýrství – Kevin Mitnick (1963 – 2023)

- Asi nejznámější sociální inženýr a hacker
- Dokázal se nabourat do desítek sociálně technických systémů
  - Získal citlivé informace
  - Zničil některá data
  - Osobní obohacení
- První „sociální“ útok ve svých 12letech (manipulace s jízdenkami MHD)
- V 16letech průnik do systémů DEC
- Kombinace sociálního inženýrství a technických a hackerských metod
- Dopaden a zatčen v roce 1993 (zajímavý proces)
- Po propuštění mu byla na 3 roky zakázána jakákoliv (moderní) komunikace kromě pevné linky
- Stal se konzultantem kyberbezpečnosti
- Napsal několik knih (doporučuji)

Sociální inženýrství – Frank Abagnale Jr.

- Známý filmem *Chyť mě, když to dokážeš* CSFD
- Je třeba představovat?
- $\Rightarrow$ Funguje sociální inženýrství ještě dnes?
- Podařil se někomu nějaký (neškodný) „kousek“?

Doporučená literatura

- Singh S. 2003. *Kniha kódů a šifer – Tajná komunikace od starého Egypta po kvantovou kryptografii.* Dokořán.
- Mitnick K. , Simon W.L. Umění klamu. Helion, 2003. ISBN 83-7361-210-6