Bezpečnosť kryptografických systémov

Stanislav Palúch

Fakula riadenia a informatiky, Žilinská univerzita

23. októbra 2010

Definition (Výpočtová bezpečnosť kryptografického systému.)

Hovoríme, že kryptosystém je výpočtovo bezpečný, ak najlepší známy algoritmus na jeho prelomenie vyžaduje aspoň N krokov, kde N je špecifikované veľmi veľké číslo.

Výpočtová a bezpodmienečná bezpečnosť

Definition (Výpočtová bezpečnosť kryptografického systému.)

Hovoríme, že kryptosystém je výpočtovo bezpečný, ak najlepší známy algoritmus na jeho prelomenie vyžaduje aspoň N krokov, kde N je špecifikované veľmi veľké číslo.
Iný prístup:
Hovoríme, že kryptosystém je výpočtovo bezpečný, ak problém jeho prelomenia je polynomiálne ekvivalentný s niektorou NP ťažkou úlohou.

Definition (Bezpodmienečná bezpečnosť kryptografického systému.)

Kryptosystém je bezpodmienečne bezpečný, ak ho nemožno prelomiť ani s nekonečným množstvom výpočtových prostriedkov.

Definition

Hovoríme, že kryptosystém $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ má perfektnú bezpečnosť, keď pomienená pravdepodobnosť javu bola vyslaná priama správa $x \in \mathcal{P}$ za predpokladu javu bola prijatá zašifrovaná správa $y \in \mathcal{C}$, sa rovná pravdepodobnosti vyslania správy x, t.j.

$$P[M = x | C = y] = P[M = x].$$

Perfektná bezpečnosť

Definition

Hovoríme, že kryptosystém $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ má perfektnú bezpečnosť, keď pomienená pravdepodobnosť javu bola vyslaná priama správa $x \in \mathcal{P}$ za predpokladu javu bola prijatá zašifrovaná správa $y \in \mathcal{C}$, sa rovná pravdepodobnosti vyslania správy x, t.j.

$$P[M = x | C = y] = P[M = x].$$

Majme cézarovskú šifru $x,\ y,\ , k \in \mathbb{Z}_{26},\ y = x \oplus_{26} k$, s rovnomerným rozdelením prvdepodobnosti kľúčov, t.j. $\forall k \in \mathbb{Z}_{26}\ P[K = k] = \frac{1}{26}$.

$$P[C = y] = \sum_{k \in \mathcal{K}} P[K = k].P[M = d_k(y)] =$$

$$\sum_{k \in \mathcal{K}} P[K = k].P[M = (y \ominus_{26} k)] =$$

$$\sum_{k \in \mathcal{K}} \frac{1}{26}.P[M = (y \ominus_{26} k)] = \frac{1}{26}.\underbrace{\sum_{k \in \mathcal{K}} P[M = (y \ominus_{26} k)]}_{=1} = \frac{1}{26}$$

$$P[C = y] = \frac{1}{26}$$

Cézarovká šifra má perfektnú bezpečnosť

$$P[C = y|M = x] = P[K = y \ominus_{26} x] = \frac{1}{26}$$

$$P[M = x|C = y] = \underbrace{\frac{P[M = x].P[C = y|M = x]}{P[C = y]}}_{\text{Bayesova veta: } P(A|B) = \frac{P(A).P(B|A)}{P(B)}} = \frac{P[M = x].\frac{1}{26}}{\frac{1}{26}} = P[M = x]$$

Theorem

Cézarovská šifra aplikovaná na jeden znak má perfektnú bezpečnosť, ak sa zakaždým použije iný kľúč s rovnomerným rozdelením pravdepodobnosti.

Theorem

Nech $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ je kryptosystém, kde $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. Potom tento systém má perfektnú bezpečnosť práve vtedy, keď každý kľúč sa používa s rovnakou pravdepodobnosťou $1/|\mathcal{K}|$ a pre každé $x \in \mathcal{P}$ a pre každé $y \in \mathcal{C}$ existuje práve jeden kľúč $k \in \mathcal{K}$ taký, že $y = e_k(x)$.

Informácia o znakoch priameho textu v zašifrovaných znakoch

Pokus $\mathbf{B} = \{b_1, b_2, \ldots, b_{26}\}$, $H(\mathbf{B}) = -\sum_{i=1}^{26} P(b_i). \log_2 P(b_i)$.
Pokus **B** predstavuje vyslanie jedného znaku priameho textu.

Pokus $\mathbf{A} = \{a_1, a_2, \ldots, a_{26}\}$, $P(a_i) = \dfrac{1}{26}$ $H(\mathbf{A}) = -\log_2(26)$.

Pokus **A** predstavuje prijatie jedného znaku zašifrovaného textu.

Informácia o znakoch priameho textu v zašifrovaných znakoch

Pokus $\mathbf{B} = \{b_1, b_2, \dots, b_{26}\}$, $H(\mathbf{B}) = -\sum_{i=1}^{26} P(b_i).\log_2 P(b_i)$.
Pokus **B** predstavuje vyslanie jedného znaku priameho textu.

Pokus $\mathbf{A} = \{a_1, a_2, \dots, a_{26}\}$, $P(a_i) = \dfrac{1}{26}$ $H(\mathbf{A}) = -\log_2(26)$.
Pokus **A** predstavuje prijatie jedného znaku zašifrovaného textu.

$H(\mathbf{B}|a_i) = -\sum_{j=1}^{26} P(b_j|a_i)\log_2 P(b_j|a_i)$

Informácia o znakoch priameho textu v zašifrovaných znakoch

Pokus $\mathbf{B} = \{b_1, b_2, \dots, b_{26}\}$, $H(\mathbf{B}) = -\sum_{i=1}^{26} P(b_i).\log_2 P(b_i)$.
Pokus **B** predstavuje vyslanie jedného znaku priameho textu.
Pokus $\mathbf{A} = \{a_1, a_2, \dots, a_{26}\}$, $P(a_i) = \dfrac{1}{26}$ $H(\mathbf{A}) = -\log_2(26)$.
Pokus **A** predstavuje prijatie jedného znaku zašifrovaného textu.

$$H(\mathbf{B}|a_i) = -\sum_{j=1}^{26} P(b_j|a_i)\log_2 P(b_j|a_i)$$

$$H(\mathbf{B}|\mathbf{A}) = \sum_{i=1}^{26} P(a_i)H(\mathbf{B}|a_i) = -\sum_{i=1}^{26} P(a_i)\sum_{j=1}^{26} P(b_j|a_i)\log_2 P(b_j|a_i)$$

Informácia o znakoch priameho textu v zašifrovaných znakoch

Pokus $\mathbf{B} = \{b_1, b_2, \dots, b_{26}\}$, $H(\mathbf{B}) = -\sum_{i=1}^{26} P(b_i). \log_2 P(b_i)$.
Pokus **B** predstavuje vyslanie jedného znaku priameho textu.

Pokus $\mathbf{A} = \{a_1, a_2, \dots, a_{26}\}$, $P(a_i) = \dfrac{1}{26}$ $H(\mathbf{A}) = -\log_2(26)$.
Pokus **A** predstavuje prijatie jedného znaku zašifrovaného textu.

$$H(\mathbf{B}|a_i) = -\sum_{j=1}^{26} P(b_j|a_i) \log_2 P(b_j|a_i)$$

$$H(\mathbf{B}|\mathbf{A}) = \sum_{i=1}^{26} P(a_i) H(\mathbf{B}|a_i) = -\sum_{i=1}^{26} P(a_i) \sum_{j=1}^{26} P(b_j|a_i) \log_2 P(b_j|a_i)$$

Ale $P(b_j|a_i) = p(b_i)$

$$H(\mathbf{B}|\mathbf{A}) = -\sum_{i=1}^{26} P(a_i) \sum_{j=1}^{26} P(b_j) \log_2 P(b_j) = \sum_{i=1}^{26} P(a_i) H(\mathbf{B}) =$$
$$= H(\mathbf{B}) \sum_{i=1}^{26} P(a_i) = H(\mathbf{B})$$

Informácia o znakoch priameho textu v zašifrovaných znakoch

Pokus $\mathbf{B} = \{b_1, b_2, \dots, b_{26}\}$, $H(\mathbf{B}) = -\sum_{i=1}^{26} P(b_i).\log_2 P(b_i)$.
Pokus **B** predstavuje vyslanie jedného znaku priameho textu.

Pokus $\mathbf{A} = \{a_1, a_2, \dots, a_{26}\}$, $P(a_i) = \dfrac{1}{26}$ $H(\mathbf{A}) = -\log_2(26)$.
Pokus **A** predstavuje prijatie jedného znaku zašifrovaného textu.

$$H(\mathbf{B}|a_i) = -\sum_{j=1}^{26} P(b_j|a_i)\log_2 P(b_j|a_i)$$

$$H(\mathbf{B}|\mathbf{A}) = \sum_{i=1}^{26} P(a_i)H(\mathbf{B}|a_i) = -\sum_{i=1}^{26} P(a_i)\sum_{j=1}^{26} P(b_j|a_i)\log_2 P(b_j|a_i)$$

Ale $P(b_j|a_i) = p(b_i)$

$$H(\mathbf{B}|\mathbf{A}) = -\sum_{i=1}^{26} P(a_i)\sum_{j=1}^{26} P(b_j)\log_2 P(b_j) = \sum_{i=1}^{26} P(a_i)H(\mathbf{B}) =$$
$$= H(\mathbf{B})\sum_{i=1}^{26} P(a_i) = H(\mathbf{B})$$

Stredná informácia o vyslanom znaku priameho textu (– o pokuse **B**) v prijatom znaku zašifrovaného textu (– v pokuse **A**) je

$$I(\mathbf{A}, \mathbf{B}) = H(\mathbf{B}) - H(\mathbf{B}|\mathbf{A}) = H(\mathbf{B}) - H(\mathbf{B}) = 0$$

Prúdové šifry

Princíp prúdovej šifry:

$x_1, x_2, \ldots, x_n, \ldots$ – prúd znakov priameho textu

$k_1, k_2, \ldots, k_n, \ldots$ – prúd kľúčov

Prúd zašifrovaných znakov bude:

$$y_1, y_2, \ldots, y_n, \cdots = E_{k_1}(x_1), E_{k_2}(x_2), \ldots, E_{k_n}(x_n), \ldots$$

Cézarovské a vigenèrovské šifry možno pozmeniť tak, že znaky abecedy si predstavíme zkódované nejakým binárnym kódom (napr. ASCII kódom) a namiesto operácie $\oplus$ vykonáme operáciu XOR po bitoch značenú symbolom $\otimes$.

XOR	0	1
0	0	1
1	1	0

Potom

$$E_k(x) = x \otimes k \quad \text{a} \quad D_k(y) = y \otimes k$$

Theorem

Binárna operácia $\otimes$ je symetrická a asociatívna na $\mathbb{Z}_2$.
Platí $x \otimes x = 0$, $x \otimes 0 = x$ pre $x \in \{0, 1\}$.

One time pad - Vernamova šifra

Abeceda $A = \mathbb{Z}_2$.

Množina kľúčov i zašifrovaných textov je $\mathbb{Z}_2$.

$x_1, x_2, \dots, x_n, \dots$ – prúd znakov priameho textu

$k_1, k_2, \dots, k_n, \dots$ – prúd kľúčov, $P(k_i = 0) = P(k_i = 1) = \dfrac{1}{2}$

$y_1, y_2, \dots, y_n, \dots$ – prúd znakov zašifrovaného textu

$$\begin{array}{cccccc}
x_1, & x_2, & x_3, & \dots, & x_i, & \dots \\
k_1, & k_2, & k_3, & \dots, & k_i, & \dots \\
y_1 = x_1 \otimes k_1, & y_2 = x_2 \otimes k_2, & y_3 = x_3 \otimes k_3, & \dots, & y_i = x_i \otimes k_i, & \dots
\end{array}$$

Ak sú kľúče $k_1, k_2, \dots, k_n, \dots$ vyberané náhodne s rovnomerným rozdelením pravdepodobnosti, niet šance na prelomenie Vernamovej šifry.
Nevýhody:

- Kľúč musí byť aspoň tak dlhý, ako je správa
- Kľúč sa nesmie použiť viac, ako raz

Získavanie náhodných postupností

- z výstupu Gieiger-Mullerovho počítača
- meranie nepravidelností silne zamestnaného servera
- meranie teplotných fluktuácií

Výsledky takýchto meraní budú síce náhodné, ale pravdepodobnosti núl a jedničiek nemusia byť rovnaké.
Jeden spôsob vyrovnávania prevdepodobností je tento:

$$\underbrace{00}_{-}\,|\,\underbrace{00}_{-}\,|\,\underbrace{10}_{1}\,|\,\underbrace{11}_{-}\,|\,\underbrace{01}_{0}\,|\,\underbrace{01}_{0}\,|\,\underbrace{00}_{-}\,|\,\underbrace{11}_{-}\,|\,\underbrace{10}_{1}\,|\,\underbrace{00}_{-}\,|\,\underbrace{10}_{1}\,|$$

Iný spôsob:
Predpoklad $P(k_i = 0) = 1/2 + \epsilon$, $P(k_i = 1) = 1/2 - \epsilon$.
Položme $z_i = k_{2i} \otimes k_{2i+1}$.

$$P(z_i = 0) = P(k_{2i} = 0).P(k_{2i+1} = 0) + P(k_{2i} = 1).P(k_{2i+1} = 1) =$$

$$\left(\frac{1}{2} + \epsilon\right)^2 + \left(\frac{1}{2} - \epsilon\right)^2 = \frac{1}{2} + 2\epsilon^2$$

Útok pri viacnásobnom použití toho istého prúdu kľúčov

Predpokladajme, že dve postupnosti znakov priameho textu

$$a_1, a_2, \dots, a_n, \dots, \quad b_1, b_2, \dots, b_n, \dots$$

boli zašifrované tý istým prúdom kľúčov $k_1, k_2, \dots, k_n, \dots$.

Kryptoanalytik dostane dva zašifrované texty $y_1, y_2, \dots, y_n, \dots,$ $z_1, z_2, \dots, z_n, \dots$ také, že

$$y_i = a_i \otimes k_i, \quad z_i = b_i \otimes k_i.$$

Kryptoanalytik si vypočíta postupnosť $w_1, w_2, \dots, w_n, \dots,$ kde $w_i = y_i \otimes z_i$. Platí:

$$w_i = y_i \otimes z_i = (a_i \otimes k_i) \otimes (b_i \otimes k_i) = (a_i \otimes b_i) \otimes (k_i \otimes k_i) = (a_i \otimes b_i) \otimes 0 = (a_i \otimes b_i)$$

Postupnosť $w_1, w_2, \dots$ je postupnosť znakov jedného priameho textu zašifrovaná postupnosťou iného priameho textu a takáto postupnosť nesie dostatok informácie na odhalenie podstanej časti oboch priamych textov a v konečnom dôsledku aj postunosti bitov kľúča.

Synchronizácia zašifrovaných textov

Kryptoanalytik zachytí dve postupnosti zašifrovaných textov

$$y_1, y_2, \dots, y_n, \dots, \quad z_1, z_2, \dots, z_n, \dots,$$

ktoré boli zašifrované tým istým prúdom kľúčov, avšak sú navzájom posunúté o d pozícií, t.j.

$$y_i = a_i \otimes k_{i+d}, \quad z_i = b_i \otimes k_i.$$

Ak vytvorí postupnosť

$$w_i = y_i \otimes z_i = (a_i \otimes k_{i+d}) \otimes (b_i \otimes k_i) = (a_i \otimes b_i) \otimes (k_{i+d} \otimes k_i),$$

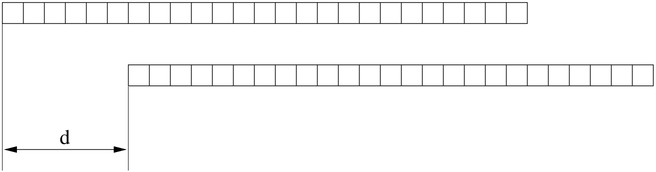
táto sa bude javiť ako postupnosť náhodných bitov.
Ak však posunie zašifrovaný text $z_1, z_2, \dots, z_n, \dots,$ oproti textu $y_1, y_2, \dots, y_n, \dots$ od d pozícií dozadu, a vytvorí postupnosť

$$w_i = y_i \otimes z_{i+d} = (a_i \otimes k_{i+d}) \otimes (b_{i+d} \otimes k_{i+d}) = (a_i \otimes b_{i+d}) \otimes (k_{i+d} \otimes k_{i+d}) = a_i \otimes b_{i+d},$$

počet núl v tejto postupnosti nápadne stúpne, lebo pravdepodobnosť nuly je pravdepodobnosťou, že $a_i = b_{i+d}$, čo sa rovná príslušnému indexu koincidencie.

Synchronizácia zašifrovaných textov

Posúvame proti sebe oba zašifrované texty. Pri zasynchronizovaní – nájdení správnej vzdialenosti *d* počet zhôd nápadne stúpne.



Použitie generátorov náhodných čísel

Lineárny kongruenčný generátor

$$X_n = (aX_{n-1} + b) \mod m$$

Perióda max $m - 1$.

Kvadratický kongruenčný generátor

$$X_n = (aX_{n-1}^2 + bX_{n-1} + c) \mod m$$

Kubický kongruenčný generátor

$$X_n = (aX_{n-1}^3 + bX_{n-1}^2 + cX_{n-1} + d) \mod m$$

Joan Boyar dokázala, že lineárny a nesjkôr aj ostatné kongruenčné generátory sú kryptograficky slabé. Nesmú sa používať v silnej kryptografii!!

Generátor RC4

Máme 256 S-boxov $S[0], S[1], \ldots, S[255]$, ktoré obsahujú niektorú permutáciu čísel 0 až 255.

```
rand()
i=i+1 mod 256
j=j+S[i] mod 256
swap(S[i],S[j])
t=(S[i]+S[j]) mod 256
k=S[t]
return k
```

Inicializačná procedúra pre RC4

Kľúč múže byť až 256*8=2048 bitov. Týmito bitmi sa naplnia postupne 8-bitové čísla $K[0], K[1], \ldots, K[255]$.

Inicializačná procedúra je takáto:

```
for i=0 to 255
{
  S[i]=i
}
j=0
for i=0 to 255
{
  j=(j+S[i]+K[i]) mod 256
  swap(S[i],S[j])
}
i=0
j=0
```

Podobné sú generátory pseudonáhodných čísel označované ako VMPC.
Je tu to isté nebezpečenstvo pri viacnásobnom používaní rovnakého kľúča ako pri Vernamovej šifre.