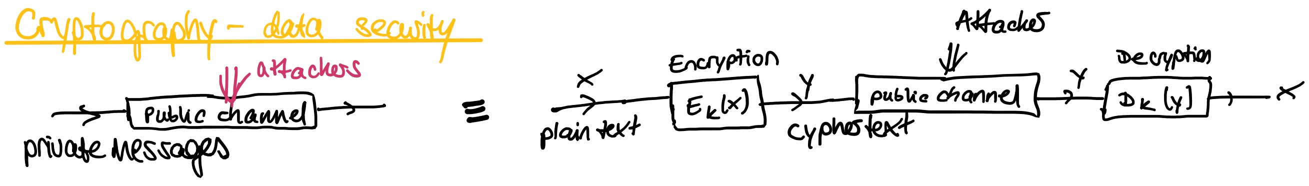
15. lecture

Mittwoch, 22. November 2023 10:19

Cryptography - data security



Attacker knows everything about system apart from a set of parameters ("key")

$E_k(x)$ → hardly invertable without "k" (key)
→ easy to invert with "k"

Type of attacks: active attack (manipulate, destroy message)

passive attack (decyphering the message (get plain text))

↳ cyphertext attack: $y_1 y_2 \cdots y_k$

↳ plaintext - cyphertext attack: $(x_1, y_1), (x_2, y_2) \dots (x_k, y_k)$

↳ chosen — " — : pick $(x_1, y_1), (x_2, y_2) \dots (x_k, y_k)$ (chose x)

Additive cypher: $y_i = x_i + k \mod (26)$ ← if using letters

HELLO + 1 = IFMMP   complexity $O(26)$
↑ size of alphabet

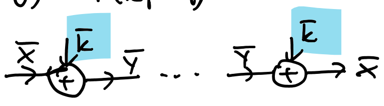
Permutation cypher: M O R N I N G = R G M I N O N
1 2 3 4 5 6 7
3 7 1 5 4 2 6

$O(n!)$ here $n = 7$

OTP - One time pad: $\bar{x} \in \{0,1\}^L$ binary vector $\bar{k} \in \{0,1\}^L$ ← random number generator

$P(k_i = 0) = P(k_i = 1) = 0.5$

$P(\bar{k}) = \frac{1}{2^L}$; $P(\bar{y}|\bar{x}) = P(\bar{x} + \bar{k} | \bar{x}) = P(\bar{k}) = \frac{1}{2^L}$ $\bar{y} = \bar{x} + \bar{k}$



⚡ ⇒ key share (secure channel necessary)

⚡ key as long as message (video ⚡)

$$P(\bar{y}) = \sum_{\bar{x} \in \{0,1\}^L} p(\bar{y}|\bar{x}) p(\bar{x}) = \frac{1}{2^L} \underbrace{\sum_{x \in \{0,1\}^L} p(\bar{x})}_{1} = \frac{1}{2^L}$$

$p(\bar{y}) = p(\bar{y}|\bar{x})$ ⇒ Statistically independent from each other $\bar{y}$ & $\bar{x}$
⇒ can never figure out $\bar{x}$
⇒ unbreakable

commutative key cryptography:

1) A: $y_A = E_{k_a}(x) \xrightarrow[\text{send}]{} B$

2) B: $y_B = E_{k_b}(y_A) = E_{k_b}(E_{k_a}(x)) \xrightarrow[\text{send}]{} A$

3) A: $y_C = D_{k_a}(y_B) = D_{k_a}(E_{k_b}(E_{k_a}(x))) = D_{k_a}(E_{k_a}(E_{k_b}(x))) = E_{k_b}(x) \xrightarrow[\text{send}]{} B$

kommutative

4) B: $D_{k_b}(y_C) = D_{k_b}(E_{k_b}(x)) = x$

⚡ 3 times over channel – channel usage bad (data speed)

Bsp.:

$\bar{k}_a$
$\bar{k}_b$

$\bar{y}_A = \bar{x} + \bar{k}_a$

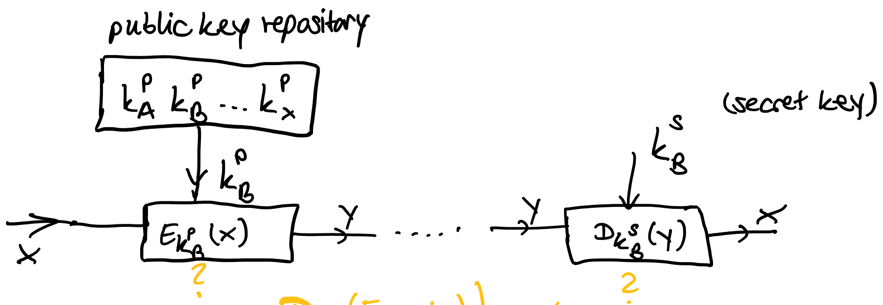
$\bar{y}_B = \bar{y}_A + \bar{k}_b = \bar{x} + \bar{k}_a + \bar{k}_b$

$\bar{y}_C = \bar{y}_B + \bar{k}_a = \bar{x} + \bar{k}_b$

$\bar{y}_A + \bar{y}_B + \bar{y}_C = \cancel{\bar{x}} + \cancel{\bar{k}_a} + \cancel{\bar{x}} + \cancel{\bar{k}_a} + \cancel{\bar{k}_b} + \bar{x} + \cancel{\bar{k}_b} = \bar{x}$

$(x^{k_a})^{k_b} = (x^{k_b})^{k_a}$

public key repository



$D_{k_B^s}(E_{k_B^p}(x)) = x$