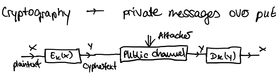
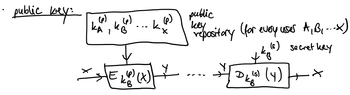
16. Lecture

Mittwoch, 29. November 2023 10:17

Cryptography → private messages over public channel



- additive cypher, permutation cypher, OTP ($\bar{y} = \bar{x} + \bar{k} \rightarrow \bar{x} = \bar{y} + \bar{k}$) adding same key (binary) $\bar{k} \in \{0,1\}^L$ $P(\bar{k}) = \frac{1}{2^L}$
- commutative key cryptography (without key sharing)
- public key:



Some results from Numbers Theory:

$a, b : a > b$ (integer) → $\exists\, q, r : a = qb + r$

How?: $q : qb \le a < (q+1)b$, $r = a - qb$

LCD $(a,b) = 1$ relative primes (largest common divides)

$\exists\, s, t : sa + tb = 1$

Fermat theorem: "p" prime "c" → $p \nmid c$ (p doesn't divide c)

$c^{p-1} = 1 \bmod p$

$c_1 \cdot 2c \cdot 3c \cdots (p-1)c$ distinct $i \neq j \Rightarrow (i-j)c \not\equiv 0 \bmod p$

$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv c \cdot 2c \cdot 3c \cdots (p-1)c$

$1 \cdot 2 \cdot 3 \cdots (p-1) = c^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1)$

Generalized Fermat theorem: $c, \underbrace{p_1, p_2}_{\text{primes}}$

$(c, p_1 p_2) = 1$ (weder p_1 noch p_2 teilen c) $c^{(p_1-1)(p_2-1)} = 1 \bmod p_1 p_2$

$\left(c^{p_1-1}\right)^{p_2-1} = 1 \bmod p_2$ $\left(c^{p_2-1}\right)^{p_1-1} = 1 \bmod p_1$

Eulers theorem: $p_1, p_2, \dots, p_r$ → $m = p_1 p_2 \cdots p_r$

$\Phi(m) = (p_1 - 1)(p_2 - 1) \cdots (p_r - 1)$ $(c, m) = 1$

$c^{\Phi(m)} = 1 \bmod m$

RSA algorithm (public key cryptography)

Choose p_1 & p_2 (large prime numbers)

$m = p_1 \cdot p_2$ $\Phi(m) = (p_1 - 1)(p_2 - 1)$ e (for public key): $(e, \Phi(m)) = 1$

d (for secret key): $d = e^{-1} \bmod \Phi(m)$

$k^{(p)} = (e, m)$ $k^{(s)} = (d, p_1, p_2)$

E & D kommutativ weil $(x^7)^8 = (x^8)^7$

x plaintext $\bar{x} = (1101\dots1)$ dec → x (integer)

y cyphertext $y = x^e \bmod m$

Decryption: $x = y^d \bmod m$

$y^d = (x^e)^d = x^{e \cdot d} = x^{q \cdot \Phi(m) + 1} = x \cdot x^{q \cdot \Phi(m)} = x \cdot \left(x^{\Phi(m)}\right)^q = x \cdot 1^q = x$ ($d = e^{-1} \bmod \Phi(m) \Rightarrow e \cdot d = q \cdot \Phi(m) + 1$; $x^{\Phi(m)} \equiv 1 \pmod m$)

Hard to crack: $m = p_1 \cdot p_2$ HARD → $\Phi(m) = (p_1 - 1)(p_2 - 1)$ $d = e^{-1} \bmod \Phi(m)$

EXAMPLE: $p_1 = 3$ $p_2 = 5$ $e = 7$

1) What is d? $m = 3 \cdot 5 = 15$ $\Phi(m) = 2 \cdot 4 = 8$ $d = 7^{-1} \bmod 8$, $d = 7$

$1 \cdot 7 \equiv 7$, $2 \cdot 7 \equiv 6$, $3 \cdot 7 \equiv 5$, $4 \cdot 7 \equiv 4$, $5 \cdot 7 \equiv 3$, $6 \cdot 7 \equiv 2$, $7 \cdot 7 \equiv 1$

2) decyphes $y = 5$

$x = y^7 \bmod 15$

$= 5^7 \bmod 15$

$= 78125 \bmod 15$

$x = 5$

How prime numbers?

$10^{150} \sim 2^{500}$ Chebyshev # of prime numbers $\le n$

$\pi(n) = \frac{n}{\log n}$ | Prob $= \frac{\pi(2^{502}) - \pi(2^{501})}{2^{502} - 2^{501}} \approx \frac{1}{350}$ → wahrs. dass in diesem Bereich eine prime numbers gefunden

$\frac{1}{175}$ (ungerade Zahlen wählen)

$2 \le b < 5$ $b_1, b_2 \dots b_5$

$b^{5-1} = 1 \bmod 5$

Common Modulus RSA

p_1, p_2 common exponent knows $m = p_1 \cdot p_2$ $\Phi(m) = (p_1 - 1)(p_2 - 1)$

$(e_A, \Phi(m)) = 1$, $(e_B, \Phi(m)) = 1$ } different for users but same primes numbers → $d_A = e_A^{-1} \bmod \Phi(m)$, $d_B = e_B^{-1} \bmod \Phi(m)$

$e_A, e_B : \exists\, s, t : s e_A + t e_B = 1 \bmod m$

same x to different users $y_A = x^{e_A}$ $y_B = x^{e_B}$

(attacker observe) y $y_A^s \cdot y_B^t = x^{s e_A + t e_B} = x^1 = x$

Digital signature

A → B $D_{k_A^{(s)}}(x) = y$

$E_{k_A^{(p)}}(y) = E_{k_A^{(p)}}\left(D_{k_A^{(s)}}(x)\right) = x$

A: $x, D_{k_A^{(s)}}(x)$

B: $x, E_{k_A^{(p)}}(y) = (x, x)$ ← received message from A (correct message) (+ from A)