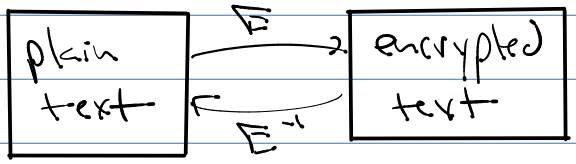
Math 321

4.6 Cryptography



Keep E & private

- Given (find) E → E^{-1} is "easy" to find : private key
  → E^{-1} is "hard" to find : public key
- Codebreaking : Cryptanalysis
  1. Given only the encrypted text → find the plain text
  2. Given encrypted plus some idea of E → find the plain text

---

Private Keys

1. Keep E secret!
2. Always know that your encrypted message has been stolen.

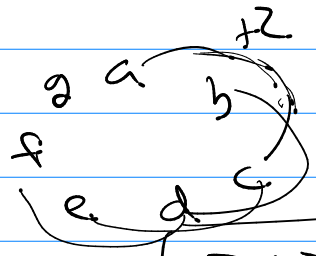
types

a) Random Replacement

alphabet: E (a,b,c,d,e ↕ c c a d b) E^{-1} plain symbols / encrypted symbols

dad $\xrightarrow{E}$ ded

b) Shift cypher



shift by K

a = 1, b = 2, ..., n ≡ # of symbols

$E(p) = (p+K) \bmod n$

$E^{-1}(c) = (c-K) \bmod n$

c) Affine Shift $\quad E(p) = (a \cdot p + k) \bmod n$

$$E^{-1}(c) = (\overline{a}(c-k)) \bmod n$$

$\overline{a}$ is a's multiplicative inverse mod n

must have $\gcd(a, n) = 1$

Ex $\quad n = 7$

symbols: a, b, c, d, e, f, g

$E(p) = (5p + 4) \bmod 7$

$E^{-1}(c) = (3(c-4)) \bmod 7$

$\gcd(7,5) = \gcd(5,2)$

$7 = 1 \cdot 5 + 2$ $\qquad 1 = 5 - 2(7-5) = 3 \cdot 5 - 2 \cdot 7$

$5 = 2 \cdot 2 + 1 \rightarrow \quad 1 = 5 - 2 \cdot 2$

d) One-Time-Pad

plain text: $p_1\ p_2\ p_3\ p_4\ \cdots\ p_m$

random int's: $s_1\ s_2\ s_3\ s_4\ \cdots\ s_m$ ← private key (one-time pad)

encrypted: $c_i = (p_i + s_i) \bmod n$

$c_k = (p_k + s_k) \bmod n$

Symbols: a, b, c, d, ␣

plain text: d ␣ a d

random int's: 1 4 1

encrypted: ␣ ␣ ␣

Public Key Crypto

Concept: ① Problem is encrypted text and the entire encryption function is known.

② Make a private key → Mixing function (privatekey) = public key

↑ used for $E()$

③ $E()$ is based on public key

$E^{-1}()$ is "hard" to find by public key

it is easy to find by private key.

RSA (locks public key crypto)

① Private key: p, q are random large primes

② Mixing: $n = p \cdot q$ (Hard: $n \to p, q$)

Secret: $m = (p-1)(q-1)$

③ Keys a) $n = pq$

b) pick any e such that $\gcd(e, m) = 1$

↑ e has a multiplicative inverse mod m

c) Find d = e's inverse mod m

④ public key (e, n)

encrypt $E(p) = p^e \bmod n$

decrypt $E^{-1}(c) = c^d \bmod n$

private: p, q, d

Running RSA/Cocks

A = 01
B = 02
⋮
M = 13
⋮
Z = 26
␣ = 27

MARK␣WAS␣HERE

1301

p_1 p_2

encrypt: $c_i = p_i^e \bmod n \rightarrow c_1, c_2, c_3, \ldots$

decrypt: $p_i = c_i^d \bmod n \rightarrow p_1, p_2, \ldots$