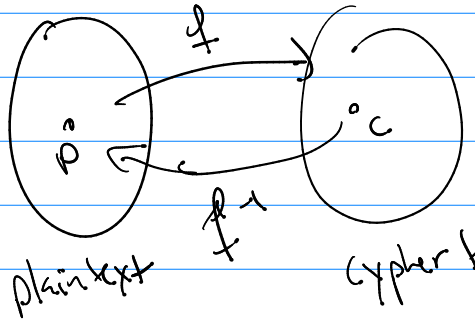
Math 321

Crypto



f: encryption func

f^{-1}: decryption fun

private key

→ Character Cypher

plain text: $p_1 p_2 p_3 p_4 \cdots p_n$ ← are characters

→ n = | characters of language |

cypher text is usually the same characters

(*) f is just a bijection from chars. to chars.

(1) shift $f(p) = (p + K) \bmod n$

Visual

a b c d e f g

$f(p) = (p+2) \bmod 7$

d ad → f c f

$f^{-1}(c) = (c-2) \bmod 7$

+5

Note →

Cryptanalysis : by study of cypher text (not "knowing" f), find plaintext.

② affine shift

$$f(p) = (ap + K) \bmod n$$

$$f^{-1}(c) = (\bar{a}(c - K)) \bmod n$$

→ $\bar{a}$ is a's inv. mod n

Ex $\gcd(a, n) = 1$ is required.

ex

0 1 2 3 4 5 6

chars: $\{a, b, c, d, e, f, g\}$ $|\text{chars}| = 7$

$$f(p) = (5p + 3) \bmod 7$$

ex 'd' → $f(3) = (5 \cdot 3 + 3) \bmod 7 = 4 \to$ 'e'

'a' → $f(0) = (5 \cdot 0 + 3) \bmod 7 = 3 \to$ 'd'

dad → ede

and $f^{-1}(c) = (\bar{5}(c - 3)) \bmod 7$

Find $\bar{5} \bmod 7$: $\gcd(7, 5)$

$\gcd(5, 2)$

$\gcd(2, 1)$

$7 = (1)5 + 2$ ← p_2

$5 = (2)2 + 1$ ← p_1

$2 = (2)1 + 0$

by p_1 $\boxed{1} = 5 + (-2)\boxed{2}$

by p_2 $1 = 5 + (-2)[7 + (-1)5]$

$1 = (3)5 + (-2)7$

$\boxed{3} = \overline{5} \bmod 7$ $\quad -2 = \overline{7} \bmod 5$

PK in our example

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

---

(3) random 1-1 replacement

$a \hookrightarrow b$
$b \hookrightarrow g$
$c \hookrightarrow c$
$d \hookrightarrow e$
$e \hookrightarrow a$
$f \hookrightarrow d$
$g \hookrightarrow f$

dad → ebe

---

(4) one-time-pad

plain text $p_1\ p_2\ p_3 \cdots p_n$

random #'s $r_1\ r_2\ r_3 \cdots r_n$

↓

cypher: $c_i = (p_i + r_i) \bmod n$

$c_1\ c_2\ c_3 \cdots c_n$

$$f^{-1}(c_i) = (c_i - r_i) \bmod n$$

Public Key RSA, Cocks cryptography

1. p, q are large primes (these are the true private key)
2. $n = pq$ $\quad M = (p-1)(q-1)$
3. pick a number, e, so that

$$\gcd(e, M) = 1$$ ← exists b/c rel. prime

4. find $d = \bar{e} \bmod M$

public (e, n) $\quad$ private (d, p, q, K)

public key

$$f(p) = p^e \bmod n$$

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

(RSA)

Do Cocks Crypto

$p = 7 \quad q = 13 \qquad n = 91 \qquad m = 72$

→ e so $\gcd(e, m) = 1$ but $e = 5$

$p = e$

Zo

$\gcd(72, 5) \qquad 72 = (14)5 + (2)$

$5 = (2)2 + \boxed{1}$

$\boxed{1} = (1)5 + (-2)(2)$

$1 = (1)5 + (-2)(72 + (-14)5)$

$1 = (29)5 + (-2)72$

$\bar{5} = 29 \pmod{72}$

$f(p) = p^5 \bmod 91$

$f^{-1}(c) = c^{29} \bmod 91$

to use this Note: $b(c \bmod 91$ we can have at most 91 symbols.

If $\bmod n$ is big..

(RSA) $\bmod 19,519$ Mark

1

1200

alt.)

$\gcd(149, 5)$

$\uparrow$ $\overline{5}$ mod 149 (as pos. int)