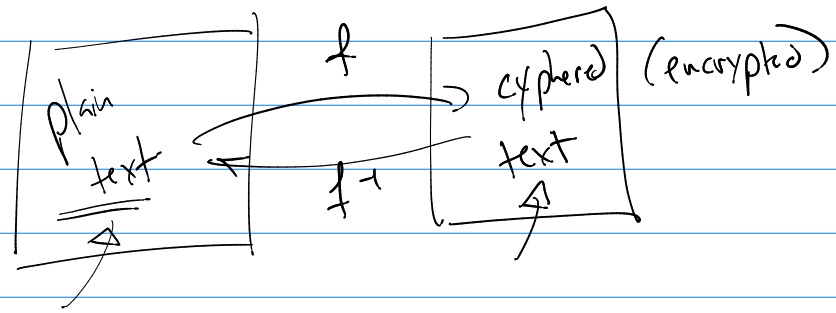
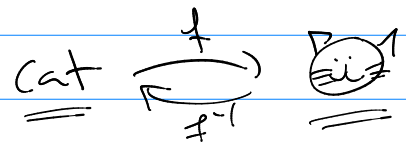
Math 321

Cryptography:



"understood" by bad guys

not "understood" by bad guys



$a \longleftrightarrow \alpha$ bijection

$b \longleftrightarrow \Delta$

$c \longleftrightarrow \beta$

$cab \xleftrightarrow{f} \beta\alpha\Delta$

for us..
Domain = Alphabet
Codomain = Alphabet

Private Key Crypto

encode: $f(p_i) = c_i$

$p_i \equiv$ plaintext elements
$c_i \equiv$ cyphered elements

If f is known then f^{-1} is trivial to find.

decode: $f^{-1}(c_i) = p_i$

ex) one-to-one bijections

Random f: $a \to q$, $b \to r$, $c \to s$, $d \to d$, $e \to a$, $f \to g$, ...

f^{-1}: $q \to a$, $r \to b$, etc

Patterns

① **Shift** $|A| = n$ (n-symbols in language)

encryption $f(p_i) = (p_i + K) \bmod n$

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

private key

(ex) $A = \{a, b, c, d, e\}$ $|A| = 5$ $K = 2$

$\quad\quad\quad\quad 0\ 1\ 2\ 3\ 4$

bad = 1, 0, 3

b	$1 \to 3$	d
a	$0 \to 2$	c
d	$3 \to 0$	a

$f(p_i) = (p_i + 2) \bmod 5$

$f^{-1}(c_i) = (c_i - 2) \bmod 5$

Note: "Strength" of a cryptosystem if $c_1, c_2, c_3, \ldots$ are known but $\boxed{\text{not}}$ the exact system ... how easy/hard is $p_1, p_2, p_3, \ldots$ to find?

② **Affine shift** $f(p_i) = (a p_i + K) \bmod n$

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

Note: $\gcd(n, a) = 1$ use Euclidean Alg. (+) Bezout's to find a^{-1}

(ex) $|A| = 12$ $f(p_i) = (35 p_i + 4) \bmod 12$

$f^{-1}(c_i) = \boxed{35}(c_i - 4) \bmod 12$

35^{-1} under mod 12

$\gcd(35, 12)$

$\gcd(12, 11)$

$35 = (2)12 + 11$

$12 = (1)11 + \boxed{1}$

$1 = 12 - 11$

$1 = 12 - (35 - 2 \cdot 12)$

$1 = 3 \cdot 12 + (-1) 35$

35^{-1}

$\ldots -13 \equiv_{12} -1 \equiv_{12} \boxed{11} \equiv_{12} 23 \equiv_{12} \ldots$ all are $35^{-1} \pmod{12}$

Strong technique: (Strongest!)

one-time-pad

$$\begin{bmatrix} a & b & c & d & \cdots \\ 0 & 1 & 2 & 3 & \cdots \end{bmatrix}$$

① $|\text{message}| = K$ create a random string of integers...

$r_1 \quad r_2 \quad r_3 \quad \cdots \quad r_K$

② $f(p_i) = (p_i + r_i) \bmod n$

so, $p_1 \quad p_2 \quad p_3 \quad p_4 \quad \cdots$

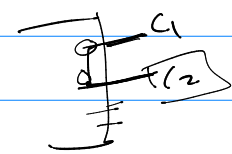
$r_1 \quad r_2 \quad r_3 \quad r_4 \quad \cdots$ ← Private Key

$p_1 + r_1, \; p_2 + r_2, \; \ldots$

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

③ $f(c_i) = (c_i - r_i) \bmod n = p_i$

Internet Issue



http

https but $f(p_i)$ and all c_i are known by bad guy!

Public Key is $f(p_i)$ is known by bad guy, but

$f^{-1}(c_i)$ is "difficult" to find from $f(p_i)$

① make private key

② "mix" private key into values to create $f(p_i)$, $\boxed{f^{-1}(c_i)}$

③ Public Key = (f, mixed key)

RSA / Codes Crypto is . .

① make p, q two large primes.

② $n = pq$ $\quad M = (p-1)(q-1)$

③ pick a number e such that $\gcd(M, e) = 1$

then $e^{-1} \bmod M$ exists. Find it.

$$d = e^{-1} \bmod M$$

④ to encrypt a message ...

$$f(p_i) = p_i^e \bmod n = C_i$$

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

$a = 00$
$b = 01$
$c = 02$
$\vdots$
$z = 25$
$\square = 26$

In use:

Message = $\boxed{S_1 S_2}\boxed{S_3 S_4}\boxed{S_5 S_6}$ - - -

you block symbols to get #'s

$\#\ \#$ $\quad$ p_1 $\quad$ p_2 $\quad$ p_3

⑤ Message = $\boxed{\text{Mark}}\boxed{\text{was}}\boxed{\text{here}}$

encrypt: $C_1 = p_1^e \bmod n \qquad C_2 = p_2^e \bmod n$

decrypt: $p_1 = C_1^d \bmod n \qquad \ldots$

public key (e, n)

private key (p, q, d)

$\boxed{\text{Ch5}}$ 5.1-5.3 prove $\forall n\, P(n)$ $n = 1, 2, 3, 4, \ldots$

Induction

tautology: $\{ P(1^{st}) \wedge \forall k \left(\left(P(1^{st}) \wedge P(2^{nd}) \wedge \cdots \wedge P(k^{th}) \right) \rightarrow P(k+1^{st}) \right) \} \rightarrow \left(\forall n\, P(n) \right)$

Basis Step: prove: $P(1^{st})$

Inductive Step: prove: $\left[P(1^{st}) \wedge P(2^{nd}) \wedge \cdots \wedge P(k^{th}) \right] \rightarrow P(k+1^{st})$