Chapter 4 – Public key

Affline cryptosystem: For each $a \in (\mathbb{Z}/N\mathbb{Z})^*$ and ~~the~~ $b \in \mathbb{Z}/N\mathbb{Z}$ is the map from $P = \mathbb{Z}/N\mathbb{Z}$ to $C = \mathbb{Z}/N\mathbb{Z}$. defined by $\boxed{C \equiv aP + b \mod N}$

Ex: Let original text = TW

$N = 26$

$A = 0, B = 1, C = 2, D = 3$ – –

$T = 19$

$a = 17, b = 20$

$\mathbb{Z}/26\mathbb{Z}$
$= 0, 1, 2$
– – 25

$(\mathbb{Z}/26\mathbb{Z})^*$
$= 1, 2, 3$ – – 25

encrypted

value of $T = \cancel{19\times}(17 \times 19 + 20) \% 26$

$= 5$

value of $W = (22 \times 19 + 20) \% 26$

$= 4$

$\boxed{TW \equiv FE}$

Enciphering key: $K_E = (a, b)$

To Decipher the code, we use ~~decipherin~~ deciphering key K_D

$C = aP + b \mod N$

$P = a^{-1}C - a^{-1}b$

$\boxed{K_D = (a^{-1}, -a^{-1}b)}$

Ex: $N = 26$

if $a = 17$, $b = 20$

$\mathbb{Z}/26\mathbb{Z} = 0, 1, 2 - - 25$

$(\mathbb{Z}/26\mathbb{Z})^* = 1, 2, 3 - - - 25$

~~cleeblefeeeb~~

$C = (17P + 20) \% 26$

Here $K_E = (17, 20)$

To find K_D : find a^{-1}

$a = 17$, $a^{-1} = 23$ since $(a\,a^{-1})_N = 1$

therefore $\Rightarrow$ $P = (23C - 23b) \bmod 26$

- In case of affine enciphering transformation of $\mathbb{Z}/N^k\mathbb{Z}$, once we know the enciphering $K_E = (a, b)$, we can compute the deciphering key $K_D = (a^{-1} \bmod N^k, -a^{-1}b \bmod N^k)$ by euclidean algo in $O(\log^3(N^k))$ bit operations

Trapdoor function = knowing the enciphering key (K_E), we ~~can~~ can compute $f: P \to C$, but we cannot compute ~~deciphering key (K_D)~~ f^{-1} without knowing extra information (such as deciphering key K_D).

Ex: Prime factoring

= easy to calculate product

= Difficult to calculate prime factors from product

= Easy to calculate one prime factor, given others.

Classical vs. Public key

- Classical ~~Classical~~ cryptosystem (private key cryptosystem) we mean a cryptosystem in which enciphering information is known, the deciphering information implemented in the same order of magnitude of time as enciphering information

If

- enciphering time were polynomial in $\log B$ and deciphering time not polynomial in $\log B$, then it is a public key.

Authentication = one of the most important ~~importants~~

Parts of message is the signature. Authentication can be done with the help of enciphering key and deciphering key.

Ex: Let F_A be the enciphering key for Alice and F_B be the enciphering key for Bob.

$\mathcal{P}$ = set of all plaintext message units
C = set of all ciphertext message units

Let $\mathcal{P} = C$

Let P = Alice's signature. It would not be enough for Alice to send Bob the encoded message $F_B(P)$ since everyone knows how to do that.
Therefore, Alice transmits $F_B F_A^{-1}(P)$. Now Bob deciphers the message using F_B^{-1}, and everything becomes plaintext except for the small jibberish $F_A^{-1}(P)$.

$F_A^{-1}(P)$ = signature of Alice and Bob applies F_A to obtain message unit P.

Hash function = A hash function is an easily computable map $\boxed{f : x \to h}$ ~~for~~ from a very long input x to much shorter output h.

Ex: The mod function is an example of hash function.

Let table-size = 17, x = value

$$\boxed{h = x \% \text{ table-size}}$$

For $x = 37599$

table-~~size~~ size = 17

$h = 37599 \% 17 = 12$

Collison

For $x = 573$

$h = 573 \% 17 = 12$

Proper choice should be an $\boxed{\text{exact power of 2}}$ for table-size to avoid too much collisons.

Key exchange : If a network of users

feel attached to traditional type of cryptosystem (private key cryptosystem), they can exchange their keys $K = (K_E, K_D)$ with another.

Ex: In the diffie-hellman key exchange, each party generates a public/private key pair and distributes the public key. After obtaining an authentic copy of each other public keys, they compute a shared secret offline.

Alice and Bob get public numbers $P = 23$, $G = 9$

Alice selects a private key $a = 4$

Bob's private key $b = 3$

Alice and Bob compute public values

$x = (9^4 \bmod 23) = \text{Alice}$

$y = (9^3 \bmod 23) = \text{Bob}$

$x = 6$

$y = 16$

Alice and Bob exchange public numbers:

Alice receives $y = 16$
Bob receives $x = 6$

Alice and Bob compute symmetric keys

$ka = y^a \bmod p = 65536 \bmod 23 = 9$
$kb = x^b \bmod p = 216 \bmod 23 = 9$

$\boxed{9 = \text{shared secret}}$

Probabilistic encryption

Deterministic encryption (plaintext encrypted into same ciphertext any time it sent) has some disadvantages:

(1) Possible to compute possibilities if plaintext message belongs to small set ("yes", "No")
(2) Difficult to prove security of the system

Therefore probabilistic encryption is used.
↓
different ciphertexts each time