3.10. Probabilistic Encryption.

In any PKC if the set of possible plaintexts is small, Eve can compute all possible ciphertexts (using Bob's public key) and compare the list to Alice's ciphertext.

Probabilistic encryption is a way around this issue:

<u>Abstract idea</u>:

- Alice has a plaintext m
- Chooses a random string of data r
- Encrypts the pair (m, r)

<u>Practically</u>: Goldwasser-Micali cryptosystem (GMCS) based on the following problem:

> Let p, q be two primes and $N = pq$
> For $a \in \mathbb{Z}$ determine whether a is a square mod N.

Bob (knows p and q).	Eve (does not know p and q)
a is a square mod N $\iff \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$	$\left(\frac{a}{N}\right) = 1 \to$ no info.

Goldwasser - Micali cryptosystem transmits one bit at a time.

Bob	Alice
Key Creation	
Choose secret primes p and q. Choose a with $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$. Publish $N = pq$ and a.	
Encryption	
	Choose plaintext $m \in \{0, 1\}$. Choose random r with $1 < r < N$. Use Bob's public key (N, a) to compute $c = \begin{cases} r^2 \bmod N & \text{if } m = 0, \\ ar^2 \bmod N & \text{if } m = 1. \end{cases}$ Send ciphtertext c to Bob.
Decryption	
Compute $\left(\frac{c}{p}\right)$. Decrypt to $m = \begin{cases} 0 & \text{if } \left(\frac{c}{p}\right) = 1, \\ 1 & \text{if } \left(\frac{c}{p}\right) = -1. \end{cases}$	

If Alice wants to send $m=0$, she sends a square mod N

if Alice wants to send $m=1$, she sends a non-square mod N

$$\left(\frac{c}{p}\right) = \begin{cases} \left(\frac{r^2}{p}\right) = \left(\frac{r}{p}\right)^2 = 1 & \text{if } m=0 \\ \left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{r}{p}\right)^2 = -1 & \text{if } m=1 \end{cases}$$

Eve: $\left(\frac{c}{N}\right) = \left(\frac{r^2}{N}\right) = \left(\frac{r}{N}\right)^2 = 1$

$$\left(\frac{c}{N}\right) = \left(\frac{ar^2}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{r}{N}\right)^2 = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\left(\frac{r}{N}\right)^2 =$$

$$= (-1)(-1)\cdot 1 = 1$$

$\Rightarrow$ no information.

Example Bob: $p = 23$, $q = 17$ – secret

$N = pq = 391$

$a = 3$

$$\left(\frac{3}{23}\right) = \left(\frac{23}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Alice • wants to send $m = 0$

- chooses a random $r = 281$
- sends ciphertext $c = r^2 \bmod N = 370 \pmod{391}$

Bob: $\left(\frac{370}{23}\right) = \left(\frac{2}{23}\right) = 1 \rightarrow m = 0$

Note: • GMCS is not practical because if N has 1000 bits then the message expansion ratio is 1000.

- But probabilistic ideas (introducing a random element) make PKC more secure.
- It is desirable to take deterministic PKC (such as RSA) and turn them into probabilistic ones.