1. Cyclic Groups

A group $G$ is cyclic if $G$ is finite and there exists an element $g$ of $G$ such that:

$$\forall a \in G, \exists n \in \mathbb{N}, a = g^n$$

Element $g$ is called a generator of group $G$.

2. Hard Problems

Most cryptographic constructions are based on hard problems. Their security is proved by reduction to these problems:

- Discrete Logarithm problem, DL: Given a group $\langle g \rangle$ and $g^x$, compute $x$.
  $$\text{Adv}^{DL}(A) = \Pr[A(g^x) \rightarrow x | x, y \leftarrow R \{1, q\}]$$

- Computational Diffie-Hellman, CDH: Given a group $\langle g \rangle$, $g^x$ and $g^y$, compute $g^{x+y}$.
  $$\text{Adv}^{CDH}(A) = \Pr[A(g^x, g^y) \rightarrow g^{x+y} | x, y \leftarrow R \{1, q\}]$$

- Decisional Diffie-Hellman, DDH: Given a group $\langle g \rangle$, distinguish between the distributions $\langle g^x, g^y, g^{x+y} \rangle$ and $\langle g^x, g^y, g^r \rangle$.
  $$\text{Adv}^{DDH}(A) = \Pr[A(g^x, g^y, g^{x+y}) \rightarrow 1 | x, y, r \leftarrow R \{1, q\}] - \Pr[A(g^x, g^y, g^r) \rightarrow 1 | x, y, r \leftarrow R \{1, q\}]$$

- RSA: Given $N = pq$ and $e \in Z^*_\phi(N)$, compute the inverse of $e$ modulo $\phi(N) = (p - 1)(q - 1)$. Factorization

2.1 Integer Factorization and RSA

- If we know $p, q$, it's easy to find $n = pq$.
- If we know $n$, it's difficult to find $p$ and $q$.
- $x \rightarrow x^e \mod n$ easy (cubic)
- $y = x^e \rightarrow x \mod n$ difficult
\[ x = y^d \text{ where } d = e^{-1} \mod \phi(n) \]

### 2.2 The Diffie-Hellman key Exchange

Let \( g \) be a generator of a cyclic group of prime order \( q \).

- \( A \rightarrow B : g^a \)
- \( B \rightarrow A : g^b \)
- \( A \rightarrow B : \{N\} g^{ab} \)

\[(g^a)^b = g^{ab} = (g^b)^a\]

- \( g \): is public.
- \( a \): is private random number generated by \( A \).
- \( b \): is private random number generated by \( B \).

### 2.3 The Relation Between the Problems

\[ \text{DL} \Rightarrow \text{CDH} \Rightarrow \text{DDH} \]

If Discreet logarithm is hard than Computational Diffie-Hellman is hard and Decisional Diffie-Hellman is hard. If we break the DL, CDH and DDH are breakable.

### 3. Idea of security Notions

#### 3.1 One-wayness(OW)

Without the private key, it is computationally impossible to recover the plain-text. (Near of Perfect Security of Shannon).

\[ \Pr_{m,r} [A(c) = m \mid c = E(m, r)] \text{ is negligible.} \]

#### 3.2 Indistinguishability(IND)

A cryptosystem is considered secure in terms of indistinguishability if no adversary \( A \), given an encryption of a message randomly chosen from a two-element message space determined by the adversary, can identify the message choice with probability significantly better than that of random guessing (1/2). If any adversary can succeed in distinguishing the chosen ciphertext with a probability significantly greater than 1/2, then this adversary is considered to have an "advantage" in distinguishing the ciphertext, and the scheme is not considered secure in terms of indistinguishability. \(^1\)

The adversary is not able to guess in polynomial-time even a bit of the plain-text knowing the cipher-text, notion introduced by S. Goldwasser and S. Micali ([GM84]). See Slides of Indistinguishability lecture 2.

\(^1\) Ciphertext indistinguishability, Wikipedia
Game Adversary: $A = (A_1, A_2)$

1. The adversary $A_1$ is given the public key $pk$.
2. The adversary $A_1$ chooses two messages $m_0, m_1$.
3. $b = 0, 1$ is chosen at random and $c = E(m_b)$ is given to the adversary.
4. The adversary $A_2$ answers $b'$.
5. The probability $Pr[b = b'] - 1$ should be negligible.

3.3 Non Malleability (NM)

The adversary should not be able to produce a new cipher-text such that the plain-texts are meaningfully related, notion introduced by D. Dolev, C. Dwork and M. Naor in 1991 ([DDN91,BDPR98,BS99]).

Example: homomorphic encryption: $\{a\}_k \times \{b\}_k = \{a \times b\}_k$

3.4 The Relation Between the Problems

Non Malleability $\Downarrow$
Indistinguishability $\Downarrow$
One-Wayness

4. Notions of Encryption Scheme Security

4.1 IND-XXX Security

An encryption scheme is IND-XXX secure, if for any adversary $A$ the function $ADV_{S,A}^{\text{IND-XXX}}$ is negligible.

4.1.1 IND-XXX Games

Given $S = (K, E, D)$, $A = (A_1, A_2)$ of polynomial-time probabilistic algorithms.

$IND^b_{XXX}(A)$ follows:
- Generate $(pk, sk) \leftarrow R K(\eta)$.
- $(s, m_0, m_1) \leftarrow R A^{O_1}(\eta, pk)$
- $b' \leftarrow R A^{O_2}(\eta, pk, s, E(pk, m_b))$
- return $b'$.

$ADV_{S,A}^{\text{IND}_{XXX}}(\eta) = Pr[b' \leftarrow R \text{ IND}^1_{XXX}(A) : b' = 1] - Pr[b' \leftarrow R \text{ IND}^0_{XXX}(A) : b' = 1]$
4.1.1.1 Example IND-CCA1 Game

Given an encryption scheme $S = (K, E, D)$. An adversary is a pair $A = (A_1, A_2)$ of polynomial-time probabilistic algorithms, $b \in \{0, 1\}$.

Let $IND_{b_{\text{CCA}}}^b (A)$ be the following algorithm:

- Generate $(pk, sk) \leftarrow^R K(\eta)$.
- $(s, m_0, m_1) \leftarrow^s A_{O_1}^1(\eta, pk)$ where $O_1 = D$
- $b' \leftarrow^R A_2 (\eta, pk, s, E(pk, m_b))$
- return $b'$.

Then, we define the advantage against the IND-CCA1 game by:

$$ADV_{S,A}^{\text{IND}_{\text{CCA1}}} (\eta) = \Pr [b' \leftarrow^R IND_{\text{CCA1}}^1 (A) : b' = 1] - \Pr [b' \leftarrow^R IND_{\text{CCA1}}^0 (A) : b' = 1]$$

4.2 The NM-XXX Games

Given $S = (K, E, D)$. An adversary $A = (A_1, A_2)$ of polynomial-time probabilistic algorithms, $m, m', m^* \in M$. Let $NM_{b_{\text{XXX}}}^b (A)$:

- Generate $(pk, sk) \leftarrow^R K(\eta)$.
- $(s, M) \leftarrow^s A_{O_1}^1(\eta, pk)$, $m_0, m_1, \leftarrow M$
- $(R, C') \leftarrow^R A_{O_2}^2 (\eta, pk, s, M, E(pk, m_b))$, $M' \leftarrow D(C')$
- return $R (m_b, M')$

Then, we define the advantage against the IND-CCA2 game by:

$$ADV_{S,A}^{\text{NM}_{\text{XXX}}} (\eta) = \Pr [R (m, M') \leftarrow^R NM_{\text{XXX}}^1 (A) : R (m, M') = 1] - \Pr [R (m, M^*) \leftarrow^R NM_{\text{XXX}}^0 (A) : R (m, M^*) = 1]$$

4.3 The Relation Between the Notions of Security

5. Prove of IND-CCA2 $\Rightarrow$ NM-CCA2 , NM-CCA1/ $\Rightarrow$ NM-CPA

- look at slides: Public Encryption- Pascal Lafourcade
- Relations Among Notions of Security for Public-key Encryption Schemes, M. BELLARE, A. DESAI, D. POINTCHEVAL, P. ROGAWAY.