0 Key Exchange

Write down the key-exchange experiment for a protocol Π with an adversary $\mathcal{A}$.

Answer: The Key-Exchange Experiment $KE^{eav}_{\mathcal{A},\Pi}(n)$ is as follows:

1. Two parties, holding 1^n security parameter execute protocol Π. this results in a transcript $trans$, containing all the messages exchanged by the parties and a key k output by each of the parties.
2. A uniform bit $b \in \{0, 1\}$ is chosen.
   - if $b = 0$ set $\hat{k} := k$
   - if $b = 1$ choose $\hat{k} \in \{0, 1\}^n$ uniformly at random
3. $\mathcal{A}$ is given the $trans$ and $\hat{k}$ and outputs a bit b'
4. $\mathcal{A}$ wins the experiment if $b' = b$.

1 El Gamal

1. Suppose you are given an El Gamal encryption for some unknown message $m \in \mathbb{G}$. Show how to construct a different ciphertext that decrypts to the same m.

   We have the El Gamal encryption for some unknown message $m \in \mathbb{G} := (R, C) := (g^r, m \cdot X^r)$ where X is the public key.

   We pick an arbitrary $r' \in \{0, 1\}$

   - $R' := R \cdot g^{r'} = g^r \cdot g^{r'} = g^{r+r'}$
   - $C' := C \cdot B^{r'} := X^{(r'+r)} \cdot m$

   On Giving (R', C') to the oracle, we we will get back, m.

2. Show that, given two El Gamal encryptions for messages $m_1, m_2 \in \mathbb{G}$, how you can construct a ciphertext that decrypts to the product $m_1 \cdot m_2$.

   We have the El Gamal encryption for some unknown message

   $m_1 \in \mathbb{G} := (R_1, C_1) := (g^{r_1}, m_1 \cdot X^{r_1})$ where X is the public key.
   $m_2 \in \mathbb{G} := (R_2, C_2) := (g^{r_2}, m_2 \cdot X^{r_2})$ where X is the public key.

   - $R_3 := R_1 \cdot R_2 = g^{r_1} \cdot g^{r_2} = g^{r_1+r_2} = g^{r_3}$

     Where r_1, r_2 are arbitrary. We define $r_3 := r_1 + r_2$, which we use to compute the following:

   - $C_3 := C_1 \cdot C_2 = (m_1 \cdot X^{r_1}) \times (m_1 \cdot X^{r_2}) = m_1 \cdot m_2 \cdot X^{r_1+r_2} = m_1 \cdot m_2 \cdot X^{r_3}$

   On Giving (R_3, C_3) to the oracle, we we will get back, $m_1 \cdot m_2$,

2 PKE

11.3 Katz/Lindell (part b)
Say a public-key encryption scheme ($\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}$) for n-bit messages is *one-way* if any PPT adversary $\mathcal{A}$ has a negligible probability of success in the following experiment:

- $\mathsf{Gen}(1^n)$ is run to obtain keys (pk, sk).
- A message $m \in \{0,1\}^n$ is chosen uniformly at random; a ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m)$ is computed.
- $\mathcal{A}$ is given pk and c, and outputs m'.
- If $m' = m$ then $\mathcal{A}$ succeeds.

Can a *deterministic* public-key encryption scheme be one-way? If not, prove impossibility; else, give a construction based on any of the assumptions introduced in this book.

Yes. A deterministic public-key encryption scheme Π can be one-way. We give the following construction for it.

CONSTRUCTION:

Let **RSA** be a public-key encryption scheme Π defined as follows.

- **Gen**: On input of a security parameter 1^n, run **RSA** to obtain N, e, and d. Where the public-key is $\langle N, e\rangle$ and private key is $\langle N, d\rangle$.
  Here N is the product of two n-bit prime numbers and ,e and d satisfy the equation $e \cdot d = 1 \ mod \ \phi(N)$
- **Enc**: On input a public key $pk = \langle N,\ e\rangle$ and a message $\in \{0,1\}$ choose $r \in \mathbb{Z}_{\mathbb{N}}^*$ where the least significant bit of r is m.
  Compute ciphertext as follows
  $$c := r^e \ mod \ N$$
- **Dec**: On input a private-key $sk = \langle N, d\rangle$ and a ciphertext c compute the r as follows.
  $$r := c^d \ mod \ N$$
  Output least significant bit of r as message m

3 Key-Exchange Protocol

Consider the following key-exchange protocol:

1. Alice chooses uniform $k, r \leftarrow_{\$} \{0,1\}^n$ and sends $s = k \oplus r$ to Bob.
2. Bob chooses $t \leftarrow_{\$} \{0,1\}^n$ and sends $u = s \oplus t$ to Alice.
3. Alice computes $w = u \oplus r$ and sends w to Bob.
4. Alice outputs k and Bob outputs $w \oplus t$.

Show that Alice and Bob have outputted the same key. Is this scheme secure? If yes, prove its security, otherwise show a concrete attack.

Bob receives the following from Alice in the first message:

- $s = k \oplus r$

Bob sends the following to Alice in the second message:

- $u = (k \oplus r) \oplus t$

Bob receives the following from Alice in the third message:

- $w := ((k \oplus r) \oplus t) \oplus r \implies w := k \oplus t$

Finally, Bob outputs $w \oplus t$ as his key

$\implies k_{Bob} := (k \oplus t) \oplus t \implies k_{Bob} = k = k_{Alice}$
$\therefore$ Alice and Bob output the same key.

The scheme is not secure, and we show the following *Man in the Middle* (MITM) attack.

Assume an eavesdropper is collecting the messages in the *trans*. The eaves dropper would have the following messages : $\langle s,\ u,\ w \rangle$ and can easily distinguish a key $\hat{k}$ as being truly random or being the actual k

This means that $\exists$ PPT Distinguisher D that distinguishes as follows:
Attack:

- Receive *trans* and $\hat{k}$
- Compute $u \oplus w := r$
- Compute $r \oplus s := k$

- If $k = \hat{k}$ output 1 else output 0

Case Analysis:

- Case $b' := 1$
  - In this case $Pr[D(KE^{eav}_{\mathcal{A},\Pi}(n) = 1)] = 1$
- Case $b' := 0$
  - In this case $Pr[D(KE^{eav}_{\mathcal{A},\Pi}(n) = 0)] = 1$

Since, the distinguisher D can distinguish between the two keys k, the Key-Exchange Protocol is not secure.

4 CPA, key-agreement

Show that a 2-message key-agreement protocol exists iff CPA-secure public-key encryption exists.

I.e., show how to construct a CPA-secure encryption scheme from any 2-message KA protocol, and vice-versa. Prove the security of your constructions.

Assumptions: We are assuming here the following points.

- We have *Alice* communicating with *Bob*, with *Alice* starting the communication.

We have the following message exchanges for a 2-message agreement protocol.

- *Alice* picks a $\mathbb{G}$ and uniformly random r_1
  - *Alice* computes a one-way function, X using r_1 as its parameter. and sends this computed element along with $\mathbb{G}$ to *Bob*
- *Bob* would too pick an uniformly random r_2 and compute another one-way function Y, which it would forward it to *Alice*.
- At the end of the conversation between *Alice*, and *Bob*, both will have the same set of parameters i.e., $\langle \mathbb{G}, A, B \rangle$

We use the above 2 key-agreement protocol, to construct some real encryption scheme $\Pi \implies$ **Gen, Enc, Dec** as follows

- **Key Generation:**
  - $\mathbb{G} \xleftarrow{\$} \{0,1\}^n$
  - Compute and send some X from the group $\mathbb{G}$
- **Challenge phase:**
  - On receiving two messages m_0, m_1, Pick a bit $b \in \{0,1\}$
  - Pick $r_2 \leftarrow \$\{0,1\}^n$
  - Compute $Y := \langle \mathbb{G}, r_2 \rangle$
  - A key k is chosen between the communicating parties from $\langle \mathbb{G}, X, Y, r_1 \rangle$.
  - Ciphertext c_b for message m_b is computed as $c_b := Enc_k(m_b)$
  - Send $\langle c_b, Y \rangle$ to *Bob*

We have $Pr[\mathcal{A}\ wins\ CPA_{Game}] = \dfrac{1}{2} + p(n))$; where $p(n)$ is non-$negl(n)$

Ideal Scheme $\tilde{\Pi}$: In this we have the same phases as the above scheme but with some slight modifications.

- **Key Generation:**
  - $\mathbb{G} \xleftarrow{\$} \{0,1\}^n$.
  - Compute and send some $X*$ from the group $\mathbb{G}$
- **Challenge phase:**
  - On receiving two messages m_0, m_1, Pick a bit $b \in \{0,1\}$
  - *Alice* picks a $\mathbb{G}$ and uniformly random r_1
  - Pick $r_2 \leftarrow \$\{0,1\}^n$
  - Compute $Y* := \langle \mathbb{G}, r_2 \rangle$
  - A uniformly random key k is chosen between the communicating party and exchanged.
  - Ciphertext c_b for message m_b is computed as $c_b := Enc_k(m_b)$

We can tell that for any $\mathcal{A}$, the probability that the $\mathcal{A}$ wins this ideal game is as follows:

$$Pr[\mathcal{A}\ wins\ \tilde{\Pi}] = \frac{1}{2} + \frac{q}{2^\lambda}$$

Where $\frac{q}{2^\lambda}$ is the probability that there occurs a collision in picking the same k over q polynomial queries.
Reduction: Since we see that the $\mathcal{A}$ can break the scheme Π, we now use it via distinguisher D to break the key selection algorithm with $\langle \mathbb{G}, X, Y, r_1 \rangle$.

- D would get access to the Oracle, which is either $\langle \mathbb{G}, X, Y, r_1 \rangle$ or truly random.
- **GEN:**
  - Select $r_1 \leftarrow \$\{0,1\}^n$
  - Compute and send $\langle \mathbb{G}, X \rangle$ to $\mathcal{A}$
    - $X := \langle \mathbb{G}, r_1 \rangle$

- **Challenge:**
  - On receiving two messages m_0, m_1, Pick a bit $b \in \{0, 1\}$
  - Pick $r_2 \leftarrow \$\{0, 1\}^n$
  - Compute $Y := \langle \mathbb{G}, r_2 \rangle$
  - Forward $\langle \mathbb{G}, X, Y, r_2 \rangle$ to the Oracle to receive the key k
  - Compute $c_b := \mathsf{Enc}_k(m_b)$ and send $\langle c_b, Y \rangle$ to $\mathcal{A}$
  - Finally, if $b = b'$ $\mathcal{A}$ wins.
- **Analysis**
  - Case 1: Pseudorandom
    - Here the view of $\mathcal{A}$ is exactly like the CPA_{game} with encryption scheme Π

      $$Pr[\mathcal{A}\ wins\ CPA_{Game}] = Pr[D(n) = 1|O = pseudorandom] = \frac{1}{2} + p(n))$$
  - Case 2: Truly Random
    - Here the view of $\mathcal{A}$ is exactly like the CPA_{game} with encryption scheme $\tilde{\Pi}$

      $$Pr[\mathcal{A}\ wins\ \tilde{\Pi}] = Pr[D(n) = 1|O = TRF] = \frac{1}{2} + \frac{q}{2^n}$$

$\therefore$ we have $Pr[D(n) = 1|O = pseudorandom] - Pr[D(n) = 1|O = TRF] = p(n) - \frac{q}{2^n}$ which is non-negligible. But that would be a contradiction to our initial assumption, hence Π is a secure scheme.