Course: Modern Cryptography

Public Key Encryption Scheme, KEM, DEM

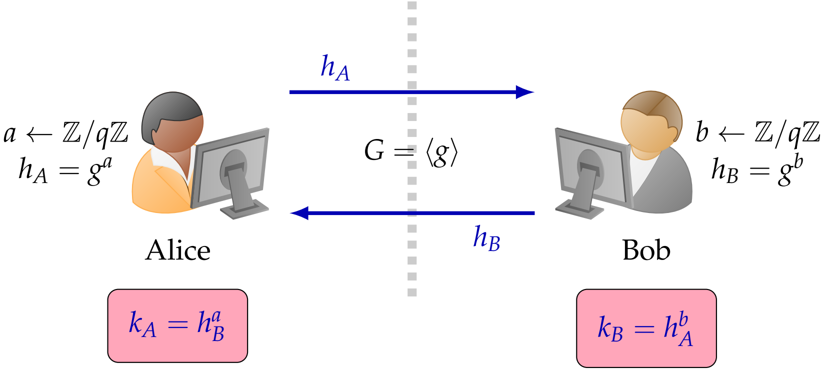
Shashank Singh

IISER Bhopal

October 30, 2025

Diffie-Hellman Key Agreement Protocol

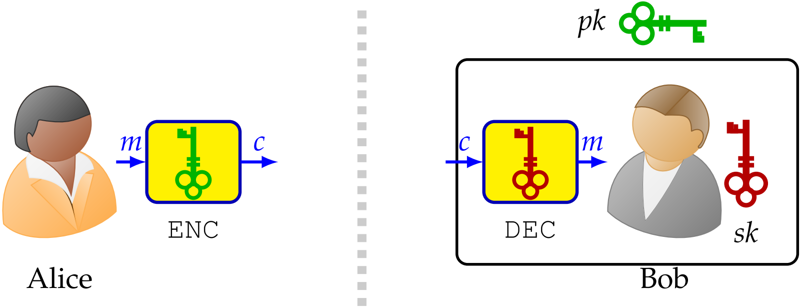
Let $(G, .)$ be a cyclic group, where DLP is known to be computationally hard. Let $G = \langle g \rangle$ and $|G| = q$.



Q1: If, it is feasible to do the key exchange. Why can't we send the whole message in the same fashion, alleviation the need of Private Key Cryptography?

☞ Diffie and Hellman also introduced in their ground-breaking work the notion of public-key (or asymmetric) cryptography.

Setting of Public Key Cryptography

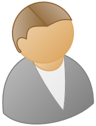


ElGamal Encryption Scheme

m

alice

$\langle G, q, g, g^x, x \rangle \leftarrow \texttt{GEN}(n)$

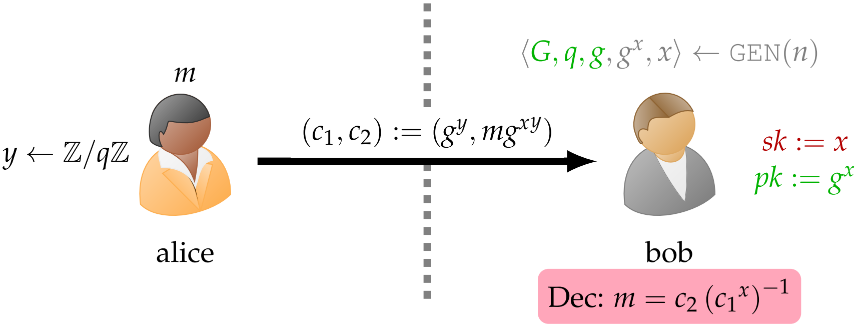


$sk := x$

$pk := g^x$

bob

ElGamal Encryption Scheme



Public-key encryption scheme

It is a triple of probabilistic polynomial-time algorithms $(\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$ such that:

- ☞ **Key-generation algorithm:** $(pk, sk) \leftarrow \texttt{GEN}(n)$, we refer pk as a public key and sk as a private key.

- ☞ **Encryption algorithm:** $c \leftarrow \texttt{ENC}_{pk}(m)$ for a $m \in \mathcal{M}$, the message space.

- ☞ **Decryption algorithm:** $\texttt{DEC}()$ takes as input a private key sk and a ciphertext c, and outputs a message m or a special symbol $\perp$ i.e., $m := \texttt{DEC}_{sk}(c)$.

It is required that, except possibly with negligible probability over (pk, sk), we have $\texttt{DEC}_{sk}(\texttt{ENC}_{pk}(m)) = m$ for any (legal) message m.

SECURITY DEFINITIONS

Given a Public-key encryption scheme $\Pi = (\mathtt{GEN}, \mathtt{ENC}, \mathtt{DEC})$ and an adversary $\mathcal{A}$, consider the following experiment:

The eavesdropping indistinguishability exp $\mathrm{PubK}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n)$**:**

- $(pk, sk) \leftarrow \mathtt{GEN}(n)$.
- $\mathcal{A}$ is given pk, and it outputs a pair of equal-length messages m_0, m_1 in the message space.
- The challenge ciphertext $c \leftarrow \mathtt{ENC}_{pk}(m_b)$, where $b \overset{\mathtt{uni}}{\leftarrow} \{0, 1\}$, is given to $\mathcal{A}$.
- $\mathcal{A}$ outputs a bit b' . The output of the experiment is 1 if $b' = b$, and 0 otherwise. If $b' = b$ we say that $\mathcal{A}$ succeeds.

Definition

A public-key encryption scheme $\Pi = (\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$ has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function ε such that

$$\Pr\left[\mathrm{PubK}^{\texttt{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \varepsilon(n)$$

Remark: Since $\mathcal{A}$ is given pk, $\mathcal{A}$ can access the encryption oracle for free.

Definition

A public-key encryption scheme $\Pi = (\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$ has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function ε such that

$$\Pr\left[\mathrm{PubK}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \varepsilon(n)$$

Remark: Since $\mathcal{A}$ is given pk, $\mathcal{A}$ can access the encryption oracle for free.

Proposition

If a public-key encryption scheme has indistinguishable encryptions in the presence of an eavesdropper, it is CPA-secure.

Theorem

If public-key encryption scheme Π is CPA-secure, then it also has indistinguishable multiple encryptions.

Remark

For public-key encryption schemes- indistinguishable encryptions in the presence of an eavesdropper, CPA-security, and indistinguishable multiple encryptions- that are all equivalent. We will simply use the term "CPA-security" to refer to schemes meeting these notions of security.

Security against Chosen-Ciphertext Attacks

The CCA indistinguishability exp $\mathrm{PubK}^{\mathtt{cca}}_{\mathcal{A},\Pi}(n)$**:**

- $(pk, sk) \leftarrow \mathtt{GEN}(n)$.
- $\mathcal{A}$ is given pk and and access to a decryption oracle $\mathtt{DEC}_{sk}(\cdot)$. It outputs a pair of equal-length messages m_0, m_1 in the message space.
- The challenge ciphertext $c \leftarrow \mathtt{ENC}_{pk}(m_b)$, where $b \overset{\mathtt{uni}}{\leftarrow} \{0, 1\}$, is given to $\mathcal{A}$.
- $\mathcal{A}$ continues to interact with the decryption oracle, but is not allowed to request a decryption of c itself.
- $\mathcal{A}$ outputs a bit b' . The output of the experiment is 1 if $b' = b$, and 0 otherwise. If $b' = b$ we say that $\mathcal{A}$ succeeds.

Definition

A public-key encryption scheme $\Pi = (\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$ has indistinguishable encryptions under a chosen-ciphertext attack (or is CCA-secure) if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function ε such that

$$\Pr\left[\mathrm{PubK}^{\texttt{cca}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \varepsilon(n)$$

Remark

If a scheme has indistinguishable encryptions under a chosen-ciphertext attack then it has indistinguishable multiple encryptions under a chosen-ciphertext attack, where this is defined appropriately.

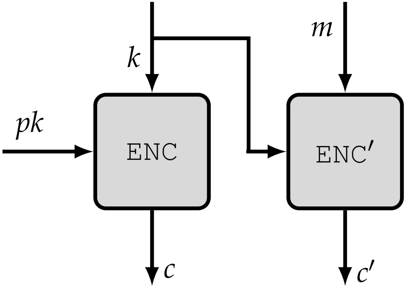
Hybrid Encryption and the KEM/DEM Paradigm

- ☞ Public key encryption schemes are much slower than the private key encryption schemes.

- ☞ It is possible to do better by using private-key encryption in tandem with public-key encryption. The resulting combination is called hybrid encryption and is used extensively in practice.

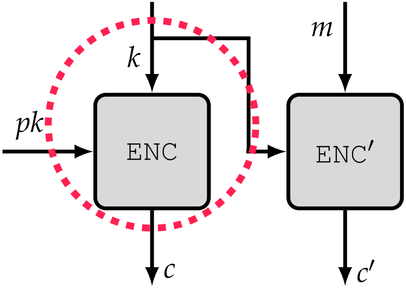
- ☞ The basic idea is to use public-key encryption to obtain a shared key k, and then encrypt the message m using a private-key encryption scheme and key k.

Hybrid Encryption..



where ENC() is a public key encryption scheme and ENC′() is a private key encryption scheme.

Hybrid Encryption..



where $\mathtt{ENC}()$ is a public key encryption scheme and $\mathtt{ENC}'()$ is a private key encryption scheme.

- A more direct hybrid approach is to use a public-key primitive called a key-encapsulation mechanism (KEM) which will be described in the next slide.

KEY-ENCAPSULATION MECHANISM (KEM)

Definition (KEM)

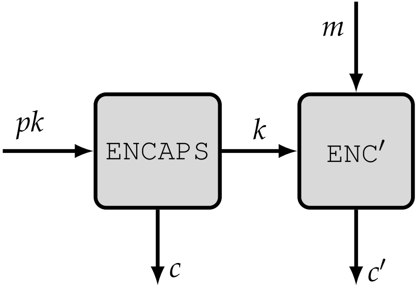
It is a tuple of PPT algorithms $(\texttt{GEN}, \texttt{ENCAPS}, \texttt{DECAPS})$ such that:

- $\texttt{GEN}()$ takes as input the security parameter 1^n and outputs a public-/private-key pair (pk, sk).
- $(c, k) \leftarrow \texttt{ENCAPS}_{pk}(n)$.
- $\perp$ or $k := \texttt{DECAPS}_{sk}(c)$.

It is required that with all but negligible probability over (sk, pk) output by $\texttt{GEN}(1^n)$, if $\texttt{ENCAPS}_{pk}(1^n)$ outputs (c, k) then $\texttt{DECAPS}_{sk}(c)$ outputs k.

- Any public-key encryption scheme trivially gives a KEM by choosing a random key k and encrypting it. As we will see, however, dedicated constructions of KEMs can be more efficient.

- Using a KEM , we can implement hybrid encryption as in Figure below.



Data-Encapsulation Mechanism (DEM)

– A private-key encryption scheme, where secret key is obtained using KEM, is called a data-encapsulation mechanism (DEM) for obvious reasons.

A Formal specification of DEM

Let $\Pi = (\texttt{GEN}, \texttt{ENCAPS}, \texttt{DECAPS})$ be a KEM with key length n, and let $\Pi' = (\texttt{GEN}', \texttt{ENC}', \texttt{DEC}')$ be a private-key encryption scheme. Construct a public-key encryption scheme $\Pi^{\text{hy}} = (\texttt{GEN}^{\text{hy}}, \texttt{ENC}^{\text{hy}}, \texttt{DEC}^{\text{hy}})$ as follows:

- $\texttt{GEN}^{\text{hy}}$: $(pk, sk) \leftarrow \texttt{GEN}(n)$.
- $\texttt{ENC}^{\text{hy}}$: on input a public key pk and a message $m \in \{0,1\}^*$,
  - Compute $(c, k) \leftarrow \texttt{ENCAPS}_{pk}(n)$.
  - Compute $c' \leftarrow \texttt{ENC}'_k(m)$.
  - Output the ciphertext $\langle c, c' \rangle$.
- $\texttt{DEC}^{\text{hy}}$: on input a private key sk and a ciphertext $\langle c, c' \rangle$,
  - Compute $k := \texttt{DECAPS}_{sk}(c)$.
  - Output the message $m := \texttt{DEC}'_k(m')$.

Definition

A key-encapsulation mechanism Π is CPA-secure if for all PPT adversaries $\mathcal{A}$ there exists a negligible function ε such that

$$\Pr\left[\mathrm{KEM}^{\mathtt{cpa}}_{\mathcal{A},\Pi}(n) = 1\right] = \frac{1}{2} + \varepsilon(n)$$

where,

$\mathrm{KEM}^{\mathtt{cpa}}_{\mathcal{A},\Pi}(n)$:

- $(pk, sk) \leftarrow \mathtt{GEN}(n)$ and $(c, k) \leftarrow \mathtt{ENCAPS}_{pk}(n)$
- A uniform bit $b \in \{0,1\}$ is chosen. If $b = 0$ set $\hat{k} := k$. If $b = 1$ then choose a uniform $\hat{k} \in \{0,1\}^n$.
- Give $(pk, c, \hat{k})$ to $\mathcal{A}$, who outputs a bit b'. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

Theorem

If Π is a CPA-secure KEM and Π' is a private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper, then Π^{hy} is a CPA-secure public-key encryption scheme.

Definition

A key-encapsulation mechanism Π is CCA-secure if for all PPT adversaries $\mathcal{A}$ there exists a negligible function ε such that

$$\Pr\left[\mathrm{KEM}^{\mathtt{cca}}_{\mathcal{A},\Pi}(n) = 1\right] = \frac{1}{2} + \varepsilon(n)$$

where,

$\mathrm{KEM}^{\mathtt{cca}}_{\mathcal{A},\Pi}(n)$:

- $(pk, sk) \leftarrow \mathtt{GEN}(n)$ and $(c, k) \leftarrow \mathtt{ENCAPS}_{pk}(n)$
- A uniform bit $b \in \{0, 1\}$ is chosen. If $b = 0$ set $\hat{k} := k$. If $b = 1$ then choose a uniform $\hat{k} \in \{0, 1\}^n$.
- Give $(pk, c, \hat{k})$ and access to oracle $\mathtt{DECAPS}_{sk}(\cdot)$ to $\mathcal{A}$. $\mathcal{A}$ is not allowed to request decapsulation of c.
- $\mathcal{A}$ outputs a bit b'. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

CCA Security of DEM

☞ If the private-key encryption scheme Π' is not CCA secure, then (regardless of the KEM used) neither is the resulting hybrid encryption scheme Π^{hy}.

Theorem

If Π *is a CCA-secure KEM and* Π' *is a CCA-secure private-key encryption scheme, then* Π^{hy} *is a CCA-secure public-key encryption scheme.*