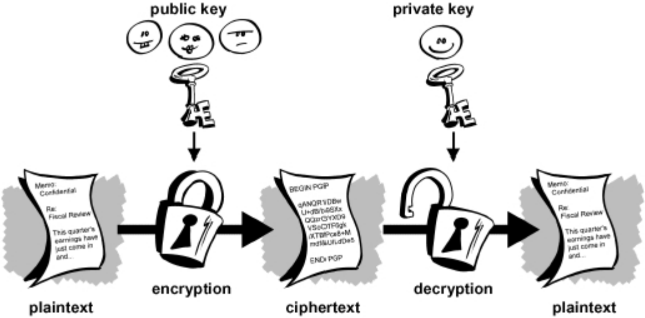
Public Key Encryption - RECAP



Public key encryption

Definition: PKE

A public-key encryption system is a **triple** of algorithms $(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ with the following properties:

- $\mathrm{KeyGen}(\lambda)$: **randomised** algorithm outputs a key pair $(\mathrm{PK}, \mathrm{SK})$. λ is a security parameter.
- $\mathrm{Enc}(\mathrm{PK}, \mathrm{m})$: **randomised** algorithm that takes $m \in \mathcal{M}$ and outputs $c \in \mathcal{C}$.
- $\mathrm{Dec}(\mathrm{SK}, \mathrm{c})$: **deterministic** algorithm that takes $c \in \mathcal{C}$ and outputs $m \in \mathcal{M}$ or $\perp$

Consistency: $\forall (PK, SK)$ output of KeyGen it holds that

$$\forall m \in M : \quad \mathrm{Dec}(\mathrm{SK}, \mathrm{Enc}(\mathrm{PK}, \mathrm{m})) = m$$

Security of PKE (IND-CPA)

The **security** of a PKE system essentially says that having the public key PK and a cipher text CT but not the secret key SK, it is *hard* to find out what is the encrypted message M (corresponding to CT).

Security for PKE (IND-CPA)

EXPERIMENT(b)

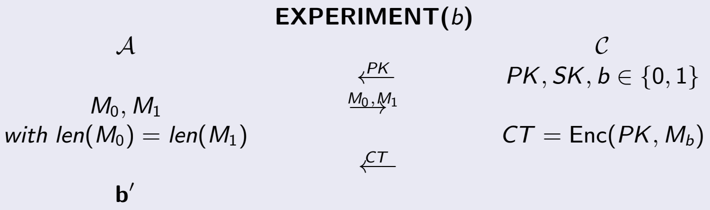
$$
\begin{array}{ccc}
\mathcal{A} & & \mathcal{C} \\
 & \xleftarrow{PK} & PK, SK, b \in \{0,1\} \\
M_0, M_1 & \xrightarrow{M_0, M_1} & \\
\textit{with } len(M_0) = len(M_1) & & CT = \text{Enc}(PK, M_b) \\
 & \xleftarrow{CT} & \\
\mathbf{b}' & &
\end{array}
$$

If $b' = b$ then $\mathcal{A}$ wins the security game (i.e. the encryption scheme is **not** secure against indistinguishability against chosen plain text attack). If $b' \neq b$, $\mathcal{A}$ has lost the security game (i.e. the scheme is secure).

Security of PKE (IND-CPA)

The **security** of a PKE system essentially says that having the public key PK and a cipher text CT but not the secret key SK, it is *hard* to find out what is the encrypted message M (corresponding to CT).

Security for PKE (IND-CPA)



EXPERIMENT(b)

$\mathcal{A}$		$\mathcal{C}$
	$\xleftarrow{PK}$	$PK, SK, b \in \{0,1\}$
M_0, M_1 *with* $len(M_0) = len(M_1)$	$\xrightarrow{M_0, M_1}$	
		$CT = \text{Enc}(PK, M_b)$
	$\xleftarrow{CT}$	
$\mathbf{b}'$		

Formal Definition - **IND-CPA :** A public-key encryption system $E = (\text{KeyGen}, \text{Enc}, \text{Dec})$ is semantically secure (IND-CPA) if for all efficient adversaries $\mathcal{A}$:

$$\text{Adv}[\mathcal{A}, E] = \Big| Pr[EXP(0) = 1] - Pr[EXP(1) = 1] \Big| < \textit{negligible}$$

Security of PKE (IND-CCA)

Chosen Cipher text **security** states that an adversary $\mathcal{A}$ should not be able to recover information about a the plain text message even if $\mathcal{A}$ can see the plain text corresponding to many cipher texts.

Security for PKE (IND-CCA)

EXPERIMENT(b)

$\mathcal{A}$		$\mathcal{C}$
	$\xleftarrow{PK}$	$PK, SK, b \in \{0, 1\}$
CCA1:C_i	$\xrightarrow{C_i}$	
$i = 1, \ldots, q$		$M_i = \mathrm{Dec}(SK, C_i)$
	$\xleftarrow{M_i}$	
CPA challenge:		
M_0, M_1	$\xrightarrow{M_0, M_1}$	
with $len(M_0) = len(M_1)$		$CT = \mathrm{Enc}(PK, M_b)$
	$\xleftarrow{CT}$	
CCA2:C_i	$\xrightarrow{C_i}$	
$i = 1, \ldots, q$		$M_i = \mathrm{Dec}(SK, C_i)$
$\mathbf{C_i \neq CT}$	$\xleftarrow{M_i}$	
$\mathbf{b'}$		

Security of PKE (IND-CCA)

Chosen Cipher text **security** states that an adversary $\mathcal{A}$ should not be able to recover information about a the plain text message even if $\mathcal{A}$ can see the plain text corresponding to many cipher texts.

Security for PKE (CCA)

If $b' = b$ then $\mathcal{A}$ wins the security game (i.e. the encryption scheme is **not** secure against chosen cipher text attack). If $b' \neq b$, $\mathcal{A}$ has lost the security game (i.e. the scheme is secure).
Formal Definition - IND-CPA : A public-key encryption system $E = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ CCA secure if for all efficient adversaries $\mathcal{A}$:

$$\mathrm{Adv}[\mathcal{A}, E] = \left| Pr[EXP(0) = 1] - Pr[EXP(1) = 1] \right| < negligible$$