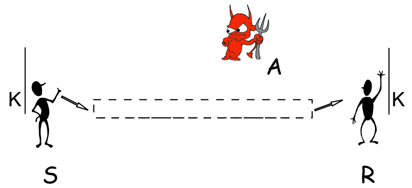
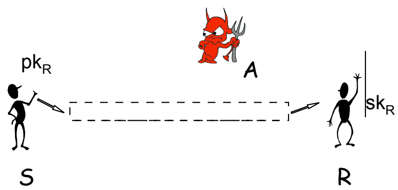
Recall: symmetric setting



1

Public-key (asymmetric) setting



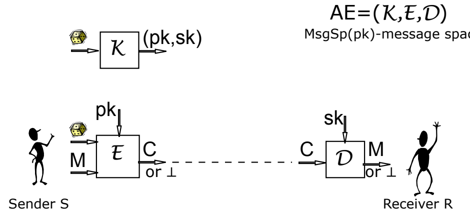
2

Asymmetric encryption schemes

A scheme AE is specified a key generation algorithm $\mathcal{K}$, an encryption algorithm $\mathcal{E}$, and a decryption algorithm $\mathcal{D}$.

AE=($\mathcal{K}$,$\mathcal{E}$,$\mathcal{D}$)

MsgSp(pk)-message space



It is required that for every (pk,sk) that can be output by $\mathcal{K}$ and every M∈MsgSp(pk), if C=$\mathcal{E}$(pk,M) then $\mathcal{D}$(sk,C)=M

3

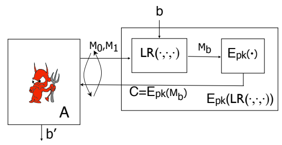
- A sender must know the receiver's public key, and must be assured that this public key is authentic (really belongs to the receiver). This is ensured be the PKI processes, which are not part of encryption.
- Unlike in a symmetric encryption, the asymmetric encryption algorithm is never stateful.
- Messages will often be group elements, encoded as bitstrings whenever necessary.

4

Indistinguishability under chosen-plaintext attacks

Fix *AE*=(K,E,D) $(pk,sk) \xleftarrow{\$} K$

For an adversary A and a bit b consider an experiment $\mathbf{Exp}^{\text{ind-cpa-}b}_{\mathcal{AE}}(A)$



The experiment returns b'

Experiment $\mathbf{Exp}^{\text{ind-cpa-}b}_{\mathcal{AE}}(A)$
$(pk, sk) \xleftarrow{\$} \mathcal{K}$
$b' \leftarrow A^{\mathcal{E}_{pk}(\mathrm{LR}(\cdot,\cdot,b))}$
Return b'

The IND-CPA advantage of A is:

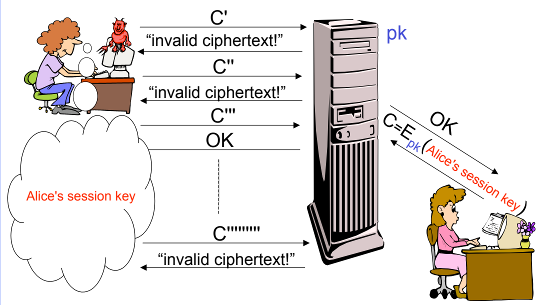
$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A) \;=\; \Pr\left[\mathbf{Exp}^{\text{ind-cpa-1}}_{\mathcal{AE}}(A)=1\right] - \Pr\left[\mathbf{Exp}^{\text{ind-cpa-0}}_{\mathcal{AE}}(A)=1\right]$$

An asymmetric encryption scheme *AE* is indistinguishable under chosen-plaintext attacks (IND-CPA secure) if for any adversary A with "reasonable" resources $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A)$ is "small" (close to 0).

5

IND-CPA is not always enough

Bleichenbacher's attack on a previous version of SSL:



6

Indistinguishability under chosen-ciphertext attacks

Fix *AE*=(K,E,D) $(pk,sk) \xleftarrow{\$} K$

For an adversary A and a bit b consider an experiment

Experiment $\mathbf{Exp}^{\text{ind-cca-}b}_{\mathcal{AE}}(A)$
$(pk, sk) \xleftarrow{\$} \mathcal{K}$
$b' \leftarrow A^{\mathcal{E}_{pk}(\mathrm{LR}(\cdot,\cdot,b)),\boxed{\mathcal{D}_{sk}(\cdot)}}$
$\boxed{\text{If } A \text{ queried } \mathcal{D}_{sk}(\cdot) \text{ on a ciphertext previously returned by } \mathcal{E}_K(\mathrm{LR}(\cdot,\cdot,b))}$
then return 0
else Return b'

The IND-CCA advantage of A is:

$$\mathbf{Adv}^{\text{ind-cca}}_{\mathcal{AE}}(A) \;=\; \Pr\left[\mathbf{Exp}^{\text{ind-cca-1}}_{\mathcal{AE}}(A)=1\right] - \Pr\left[\mathbf{Exp}^{\text{ind-cca-0}}_{\mathcal{AE}}(A)=1\right]$$

An asymmetric encryption scheme *AE* is indistinguishable under chosen-ciphertext attacks (IND-CCA secure) if for any adversary A with "reasonable" resources $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A)$ is "small" (close to 0).

7

- IND-CCA ⇒ IND-CPA
- In the literature you can meet the definitions where an adversary makes a single query to the LR encryption oracle.
- Theorem 1. Let *AE*=(K,E,D) be an asymmetric encryption scheme. Let B be an ind-cpa adversary who makes at most q queries to its LR encryption oracle. Then there exists an ind-cpa adversary A with the same running time making at most 1 query to its LR encryption oracle and such that
- $$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(B) \;\le\; q_e \cdot \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A)$$
- Theorem 2. Let B be an ind-cca adversary who makes at most q queries to its LR encryption oracle. Then there exists an ind-cca adversary A making at most one query to its LR encryption oracle, the same number of decryption queries and having the same running time such that

$$\mathbf{Adv}^{\text{ind-cca}}_{\mathcal{AE}}(B) \;\le\; q_e \cdot \mathbf{Adv}^{\text{ind-cca}}_{\mathcal{AE}}(A)$$

8

- <u>Proof of Th. 2.</u> (Th. 1 easily follows from Th. 2)

The proof uses a hybrid argument.

We will consider q experiments associated with B:

$\mathbf{Exp}^{0}_{\mathcal{AE}}(B)$, $\mathbf{Exp}^{1}_{\mathcal{AE}}(B)$, $\ldots$, $\mathbf{Exp}^{q}_{\mathcal{AE}}(B)$

We define $P(i) = \Pr\left[\mathbf{Exp}^{i}_{\mathcal{AE}}(B) = 1\right]$ and will make it s.t.

$$P(0) = \Pr\left[\mathbf{Exp}^{\text{ind-cca-0}}_{\mathcal{AE}}(B) = 1\right]$$
$$P(q) = \Pr\left[\mathbf{Exp}^{\text{ind-cca-1}}_{\mathcal{AE}}(B) = 1\right]$$

and hence $\mathbf{Adv}^{\text{ind-cca}}_{\mathcal{AE}}(B) = P(q) - P(0)$

$$= P(q) + \sum_{i=1}^{q-1}[P(i) - P(i)] - P(0)$$
$$= \sum_{i=1}^{q} P(i) - \sum_{i=0}^{q-1} P(i)$$

9

We will construct ind-cca-adversary A so that

$$\Pr\left[\mathbf{Exp}^{\text{ind-cca-1}}_{\mathcal{AE}}(A) = 1\right] = \frac{1}{q} \cdot \sum_{i=1}^{q} P(i)$$
$$\Pr\left[\mathbf{Exp}^{\text{ind-cca-0}}_{\mathcal{AE}}(A) = 1\right] = \frac{1}{q} \cdot \sum_{i=0}^{q-1} P(i)$$

and thus $\mathbf{Adv}^{\text{ind-cca}}_{\mathcal{AE}}(A) = \frac{1}{q} \cdot \mathbf{Adv}^{\text{ind-cca}}_{\mathcal{AE}}(B)$

10

Oracle $\mathcal{HE}^{\,i}_{pk}(M_0, M_1)$
- $j \leftarrow j + 1$
- If $j \leq i$
  - then $C \stackrel{\$}{\leftarrow} \mathcal{E}_{pk}(M_1)$
  - else $C \stackrel{\$}{\leftarrow} \mathcal{E}_{pk}(M_0)$
- EndIf
- Return C

Experiment $\mathbf{Exp}^{i}_{\mathcal{AE}}(B)$
- $(pk, sk) \stackrel{\$}{\leftarrow} \mathcal{K}$
- $d \leftarrow B^{\mathcal{HE}^{\,i}_{pk}(\cdot,\cdot),\mathcal{D}_{sk}(\cdot)}(pk)$
- Return d

Note that $\mathcal{HE}^{\,0}_{pk}(\cdot,\cdot) \equiv \mathcal{E}_{pk}(\mathrm{LR}(\cdot,\cdot,0))$ and $\mathcal{HE}^{\,q}_{pk}(\cdot,\cdot) \equiv \mathcal{E}_{pk}(\mathrm{LR}(\cdot,\cdot,1))$

and therefore $P(0) = \Pr\left[\mathbf{Exp}^{\text{ind-cca-0}}_{\mathcal{AE}}(B) = 1\right]$

$$P(q) = \Pr\left[\mathbf{Exp}^{\text{ind-cca-1}}_{\mathcal{AE}}(B) = 1\right]$$

11

Adversary $A^{\mathcal{E}_{pk}(\mathrm{LR}(\cdot,\cdot,b)),\mathcal{D}_{sk}(\cdot)}(pk)$
- $j \leftarrow 0$; $I \stackrel{\$}{\leftarrow} \{1, \ldots, q\}$
- Subroutine $\mathcal{OE}(M_0, M_1)$
  - $j \leftarrow j + 1$
  - If $j < I$ then $C \stackrel{\$}{\leftarrow} \mathcal{E}_{pk}(M_1)$ EndIf
  - If $j = I$ then $C \stackrel{\$}{\leftarrow} \mathcal{E}_{pk}(\mathrm{LR}(M_0, M_1, b))$ EndIf
  - If $j > I$ then $C \stackrel{\$}{\leftarrow} \mathcal{E}_{pk}(M_0)$ EndIf
  - Return C
- End Subroutine
- $d \stackrel{\$}{\leftarrow} B^{\mathcal{OE}(\cdot,\cdot),\mathcal{D}_{sk}(\cdot)}(pk)$
- Return d

$$\Pr\left[\mathbf{Exp}^{\text{ind-cca-1}}_{\mathcal{AE}}(A) = 1 \mid I = i\right] = P(i) \qquad \Pr\left[\mathbf{Exp}^{\text{ind-cca-0}}_{\mathcal{AE}}(A) = 1 \mid I = i\right] = P(i-1)$$

$$\Pr\left[\mathbf{Exp}^{\text{ind-cca-1}}_{\mathcal{AE}}(A) = 1\right] = \sum_{i=1}^{q} \Pr\left[\mathbf{Exp}^{\text{ind-cca-1}}_{\mathcal{AE}}(A) = 1 \mid I = i\right] \cdot \Pr[I = i] = \sum_{i=1}^{q} P(i) \cdot \frac{1}{q}$$

$$\Pr\left[\mathbf{Exp}^{\text{ind-cca-0}}_{\mathcal{AE}}(A) = 1\right] = \sum_{i=1}^{q} \Pr\left[\mathbf{Exp}^{\text{ind-cca-0}}_{\mathcal{AE}}(A) = 1 \mid I = i\right] \cdot \Pr[I = i] = \sum_{i=1}^{q} P(i-1) \cdot \frac{1}{q}$$
$$= \sum_{i=0}^{q-1} P(i) \cdot \frac{1}{q}$$

12

The ElGamal scheme

- Let G be a cyclic group of order n and let g be a generator of G. The ElGamal encryption scheme $EG=(\mathcal{K}, \mathcal{E}, \mathcal{D})$ associated to G,g is as follows:

Algorithm $\mathcal{K}$	Algorithm $\mathcal{E}_X(M)$	Algorithm $\mathcal{D}_x((Y,W))$
$x \xleftarrow{\$} \mathbf{Z}_n$	If $M \notin G$ then return $\perp$	$K \leftarrow Y^x$
$X \leftarrow g^x$	$y \xleftarrow{\$} \mathbf{Z}_n$; $Y \leftarrow g^y$	$M \leftarrow WK^{-1}$
Return (X,x)	$K \leftarrow X^y$; $W \leftarrow KM$	Return M
	Return (Y,W)	

- Security depends on the choice of G.

13

The ElGamal scheme in $\mathbf{Z}_\mathbf{p}^*$ for a prime p

- In this group the ElGamal is IND-CPA insecure, namely there exists an adversary A with ind-cpa advantage 1.
- The idea: given a ciphertext A can compute $J_p(M)$.

Adversary $A^{\mathcal{E}_X(\mathrm{LR}(\cdot,\cdot,b))}(X)$
$M_0 \leftarrow 1$; $M_1 \leftarrow g$
$(Y,W) \xleftarrow{\$} \mathcal{E}_X(\mathrm{LR}(M_0,M_1,b))$
If $X^{(p-1)/2} \equiv -1 \pmod p$ and $Y^{(p-1)/2} \equiv -1 \pmod p)$
then $s \leftarrow -1$ else $s \leftarrow 1$
EndIf
If $W^{(p-1)/2} \equiv s \pmod p$ then return 0 else return 1 EndIf

$J_p(W) = J_p(K) \cdot J_p(M_b) = s \cdot J_p(M_b)$

Note that M_0 is a square and M_1 is not. Why?

If b=0 then $J_p(M_0)=1$, $J_p(W)=s$, if b=1 then $J_p(M_1)=-1$, $J_p(W)\neq s$

Hence $\Pr\left[\mathbf{Exp}_{EG}^{ind-cpa-1}(A)=1\right]=1$ and $\Pr\left[\mathbf{Exp}_{EG}^{ind-cpa-0}(A)=1\right]=0$

14

- The ElGamal is IND-CPA secure in groups where the Decisional Diffie-Hellman (DDH) problem is hard,
  - i.e. in QR($\mathbf{Z}_\mathbf{p}^*$) -the subgroup of quadratic residues of $\mathbf{Z}_\mathbf{p}^*$ where p=2q+1 and p,q are primes. It's a cyclic group of prime order.

15

IND-CCA insecurity of ElGamal

- ElGamal is not IND-CCA secure regardless of the choice of group G.

Adversary $A^{\mathcal{E}_X(\mathrm{LR}(\cdot,\cdot,b)),\mathcal{D}_x(\cdot)}(X)$
Let M_0, M_1 be any two distinct elements of G
$(Y,W) \xleftarrow{\$} \mathcal{E}_X(\mathrm{LR}(M_0,M_1,b))$
$W' \leftarrow Wg$
$M \leftarrow \mathcal{D}_x((Y,W'))$
If $M = M_0 g$ then return 0 else return 1

$$M = \mathcal{D}_x((Y,W')) = K^{-1}W' = K^{-1}Wg = M_b g$$

- The ind-cca advantage of A is 1 and A maks just one LR encryption and 1 decryption query and makes 2 group multiplications.

16

Cramer-Shoup encryption scheme

- The scheme is somewhat similar to ElGamal, but uses more exponentiations and a hash function.
  - The Cramer-Shoup scheme is IND-CCA secure if the DDH problem is hard in the group and if the hash function family is universal one-way.
  - Reference: R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack", In proceedings of Crypto '98.