Recall: symmetric setting

Public-key (asymmetric) setting

Asymmetric encryption schemes

A scheme $AE$ is specified a key generation algorithm $K$, an encryption algorithm $E$, and a decryption algorithm $D$. $AE=(K,E,D)$

It is required that for every $(pk,sk)$ that can be output by $K$ and every $M \in \text{MsgSp}(pk)$, if $C=E(pk,M)$ then $D(sk,C)=M$.
• 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 by 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 numbers or group elements, encoded as bitstrings whenever necessary.

Indistinguishability under chosen-plaintext attacks

Fix an encryption scheme $AE=(K,E,D)$

Pick keys $(pk,sk)$ by running $K$

For an adversary $A$ and a bit $b$ consider two experiments $Exp$-ind-cca-$b$ $(AE,A)$, for $b=0$ or $b=1$

The difference between probabilities of outputting 0 in two experiments is called ind-cca-advantage of $A$ in attacking $AE$.

An asymmetric encryption scheme $AE$ is indistinguishable under chosen-plaintext attacks (IND-CPA secure) if ind-cca-advantage of any adversary with “reasonable” resources is “close” to 0.

IND-CPA is not always enough

Bleichenbacher’s attack on a previous version of SSL:

C’
“invalid ciphertext!”

C''
“invalid ciphertext!”

C'''
OK

A is not allowed to query its decryption oracle on ciphertexts returned by its LR encryption oracle

The difference between probabilities of outputting 0 in two experiments is called ind-cca-advantage of $A$ in attacking $AE$.

A symmetric encryption scheme $SE$ is indistinguishable under chosen-ciphertext attacks (IND-CCA secure) if ind-cca-advantage of any adversary with “reasonable” resources is “close” to 0.
IND-CCA ⇒ IND-CPA

- IND-CCA secure schemes guarantee security against more powerful adversaries.
- Any IND-CCA scheme is also IND-CPA.
- But an IND-CPA scheme is not necessarily IND-CCA.

The ElGamal scheme

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

  - Algorithm $K$
    - $x \leftarrow Z_n$
    - $X \leftarrow g^x$
    - Return $(X, x)$
  - Algorithm $E_X(M)$
    - If $M \not\in G$ then return $\perp$
    - $y \leftarrow Z_n$; $Y \leftarrow g^y$
    - $K \leftarrow X^y$; $W \leftarrow K M$
    - Return $(Y, W)$
  - Algorithm $D_k((Y, W))$
    - $K \leftarrow Y^x$
    - $M \leftarrow W K^{-1}$
    - Return $M$

- Security depends on the choice of G.

The ElGamal scheme in $\mathbb{Z}_p^*$ 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 $A^{E_X(LR(\cdot, \cdot))(X)}$
  - $M_0 \leftarrow 1$; $M_1 \leftarrow g$
  - $(Y, W) \leftarrow E_X(LR(M_0, M_1, b))$
  - If $X(g-1)/2 \equiv -1 \pmod{p}$ and $Y(g-1)/2 \equiv -1 \pmod{p}$
  - then $s \leftarrow 1$ else $s \leftarrow 1$
  - EndIf
  - If $W(g-1)/2 \equiv s \pmod{p}$ 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 $Pr[Exp^{ind-cpa-1}_{EG}(A) = 1] = 1$ and $Pr[Exp^{ind-cpa-0}_{EG}(A) = 1] = 0$

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

- Proof.
IND-CCA insecurity of ElGamal

- ElGamal is not IND-CCA secure regardless of the choice of group G.
- Adversary $A^{E_X(LR(\cdot, b)), D_\lambda(\cdot)}(X)$
  - Let $M_0, M_1$ be any two distinct elements of $G$
  - $(Y, W) \leftarrow E_X(LR(M_0, M_1, b))$
  - $W' \leftarrow Wg$
  - $M \leftarrow D_\lambda((Y, W'))$
  - If $M = M_0g$ then return 0 else return 1
  - $M = D_\lambda((Y, W')) = K^{-1}W' = K^{-1}Wg = M_0g$
- The ind-cca advantage of A is 1 and A makes just one LR encryption and one decryption oracle queries and makes 2 group multiplications.

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.