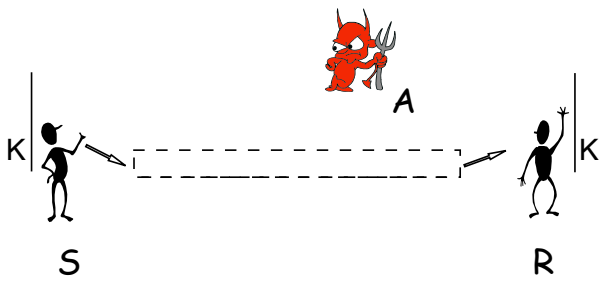
CS 4803
Computer and Network Security

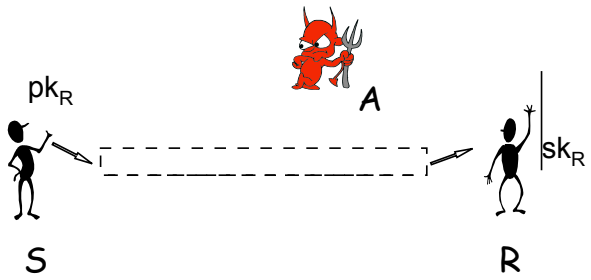
Alexandra (Sasha) Boldyreva

Public-key encryption

Recall: symmetric setting



Public-key (asymmetric) setting

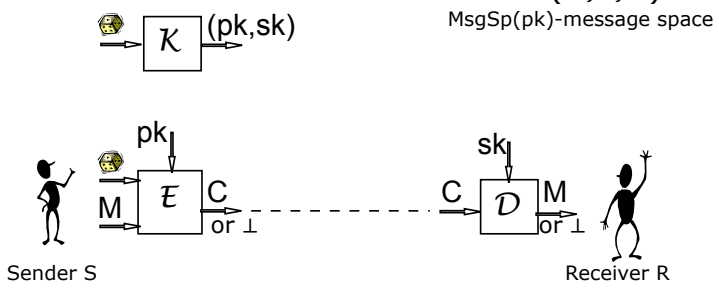


Asymmetric encryption schemes

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 $M \in MsgSp(pk)$, if $C=\mathcal{E}(pk,M)$ then $\mathcal{D}(sk,C)=M$

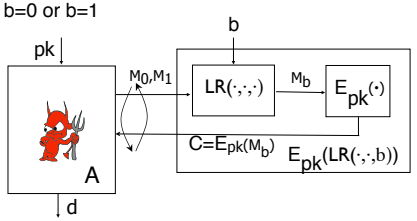
- A sender must know the receiver's public key, and must be assured that this public key is authentic (really belongs to the receiver). This is ensured be the PKI processes, which are not part of encryption.
- Unlike in a symmetric encryption, the asymmetric encryption algorithm is never stateful.
- Messages will often be 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-cpa-b (AE,A), for b=0 or b=1

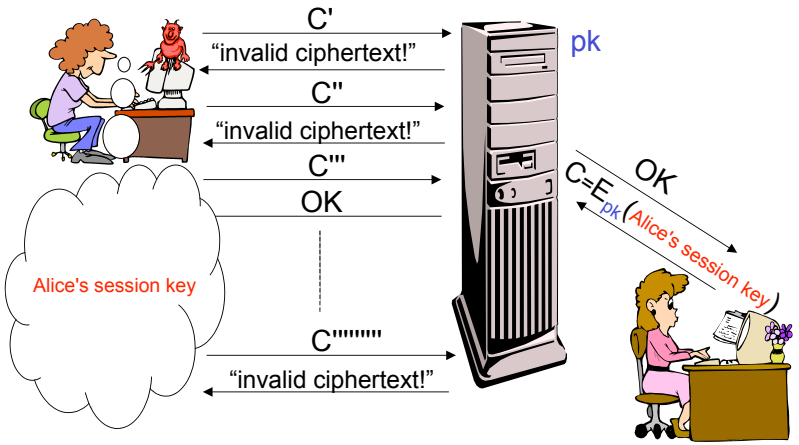


The difference between probabilities of outputting 0 in two experiments is called ind-cpa-advantage of A in attacking AE.

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:

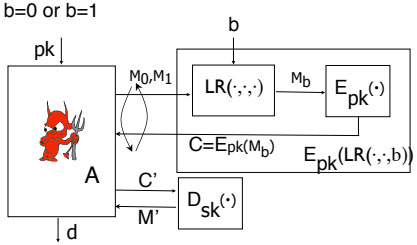


Indistinguishability under chosen-ciphertext attacks

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



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 SE.

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

The ElGamal scheme in $\mathbf{Z}_p^*$ 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 $A^{\mathcal{E}_X(\mathrm{LR}(\cdot,\cdot,b))}(X)$
$M_0 \leftarrow 1$; $M_1 \leftarrow g$
$(Y, W) \xleftarrow{\$} \mathcal{E}_X(\mathrm{LR}(M_0, M_1, b))$
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 $\Pr\left[\mathbf{Exp}_{EG}^{ind-cpa-0}(A)=1\right]=0$

- Theorem. The ElGamal is IND-CPA secure in groups where the Decisional Diffie-Hellman (DDH) problem is hard,
  - i.e. in $QR(\mathbf{Z}_p^*)$ -the subgroup of quadratic residues of $\mathbf{Z}_p^*$ 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 $A^{\mathcal{E}_X(\mathrm{LR}(\cdot,\cdot,b)),\mathcal{D}_x(\cdot)}(X)$
- 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 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.
  - Reference: R. Cramer and V. Shoup, “A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack”, In proceedings of Crypto ‘98.