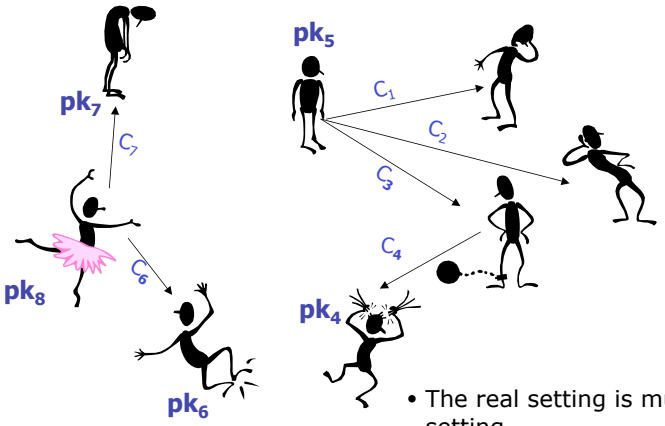
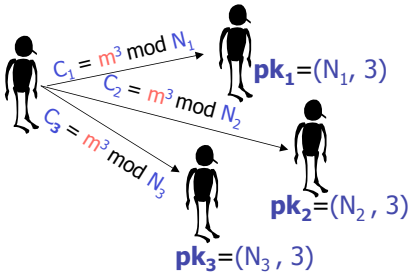
- We studied several definitions of security of asymmetric encryption schemes (IND-CPA, IND-CCA).
- Recall that the definitions consider a single user (a person with a public key).
- This "single-user" setting is different from practice

Real world is more complex



- The real setting is multi-user setting
- Are provably secure schemes really secure in this setting?

Recall: Håstad-type attack on RSA



$C_1, C_2, C_3, pk_1, pk_2, pk_3$

If N_1, N_2, N_3 are relatively prime then by Chinese Remainder Theorem can combine

$$\begin{cases} C_1 = m^3 \bmod N_1 \\ C_2 = m^3 \bmod N_2 \\ C_3 = m^3 \bmod N_3 \end{cases}$$

to find $C = m^3 \bmod N_1 N_2 N_3$

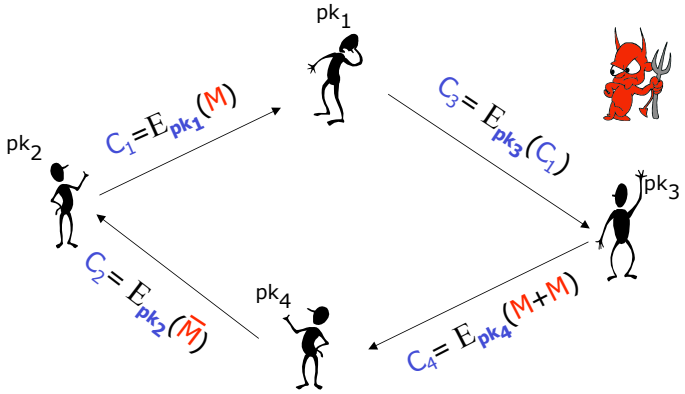
Since $m^3 < N_1 N_2 N_3$ then

$m \leftarrow \sqrt[3]{C}$

- Under the RSA assumption the Plain RSA is one-way in the single-user setting
- But it is not one-way in the multi-user setting

- Plain RSA:
  Can't recover plaintexts in the single user setting.
  Can recover plaintexts in the multi-user setting.
- RSA-OAEP:
  No info about plaintexts is leaked in the single user setting.
  Is any info about plaintexts leaked in the multi-user setting?
- Are the "provably-secure" schemes really secure in the practical (multi-user) setting?
- The reassuring answer is that given "good" definitions of security (i.e. IND-CPA, IND-CCA) security in the single-user setting implies security in the multi-user setting.

Towards a definition for the multi-user setting

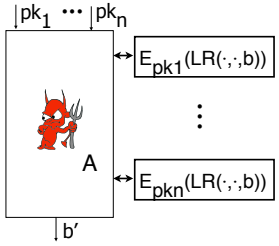


Danger: the adversary can see encryptions of related messages under different public keys.

IND-CPA security in the multi-user setting.

Fix *AE*=(K,E,D) $(pk1,sk1) \xleftarrow{\$} K$ ... $(pkn,skn) \xleftarrow{\$} K$

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



Resources of A are the running time and the max number of queries to each oracle

The experiment returns b′

The n-IND-CPA advantage of A is:

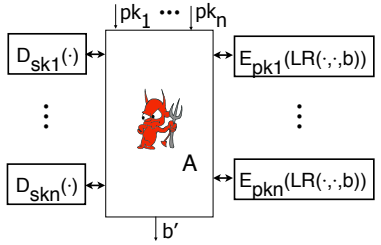
$$\mathbf{Adv}_{AE}^{n\text{-}ind\text{-}cpa}(A) = \Pr\left[\mathbf{Exp}_{AE}^{n\text{-}ind\text{-}cpa\text{-}1}(A) = 1\right] - \Pr\left[\mathbf{Exp}_{AE}^{n\text{-}ind\text{-}cpa\text{-}0}(A) = 1\right]$$

An asymmetric encryption scheme *AE* is IND-CPA secure in the multi-user setting if for any adversary *A* with "reasonable" resources $\mathbf{Adv}_{AE}^{n\text{-}ind\text{-}cpa\text{-}b}(A)$ is "small" (close to 0).

IND-CCA security in the multi-user setting.

Fix *AE*=(K,E,D) $(pk1,sk1) \xleftarrow{\$} K$ ... $(pkn,skn) \xleftarrow{\$} K$

For an adversary *A* and a bit b consider an experiment $\mathbf{Exp}_{AE}^{n\text{-}ind\text{-}cpa\text{-}1}(A)$



A is not allowed to query a decryption oracle on a ciphertext returned by the corresponding LR encryption oracle

Resources of A are the running time, the max number of queries to each LR oracle and the max number of queries to each decryption oracle

The experiment returns b′

The n-IND-CCA-mu advantage of A is:

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

An asymmetric encryption scheme *AE* is IND-CCA secure in the multi-user setting if for any adversary A with "reasonable" resources $\mathbf{Adv}_{AE}^{n\text{-}ind\text{-}cca\text{-}b}(A)$ is "small" (close to 0).

General reduction

- Theorem. Let *AE* be an asymmetric encryption scheme. For any adversary *A* there exists an adversary *B* with similar running time but who does only 1 query to its LR oracle such that
- $$\mathbf{Adv}_{AE}^{n\text{-}ind\text{-}cpa}(A) \leq n \cdot q_e \cdot \mathbf{Adv}_{AE}^{ind\text{-}cpa}(B)$$
- A similar statement can be made for the case of chosen-ciphertext attacks.
- Proof uses hybrid argument.
- The theorem implies that a scheme secure in the single-user setting is also secure in the multi-user setting.
- It shows, however, that security degrades as we add more users and allow users to encrypt more data.

The need for concrete security improvements

- Consider a public-key encryption scheme such that ind-cpa advantage of any polynomial-time adversary is less than 2^{-60}
- Assume in a real setting the number of users n=200 000 000.
- Allow $q_e=2^{30}$ messages be encrypted under each public key.
- Then n-ind-cpa advantage can be 0.2, which is not good.

- But maybe there is a better reduction?
- No, security loss cannot be prevented in general as there exists an encryption scheme for which the drop in security in the multi-user setting is $q_e \cdot n$
- However, we can hope to do better for specific schemes.

ElGamal in the multi-user setting

- General reduction implies that for any *A* there exists *B** s.t.
- $$\mathbf{Adv}_{EG}^{n\text{-}ind\text{-}cpa}(A) \leq n \cdot q_e \cdot \mathbf{Adv}_{EG}^{ind\text{-}cpa}(B)$$
- Theorem [improved reduction]. For any *A* there exists *B** with similar resources s.t.
- $$\mathbf{Adv}_{EG}^{n\text{-}ind\text{-}cpa}(A) \leq \mathbf{Adv}_{EG}^{ind\text{-}cpa}(B)$$

* B runs in time similar to that of A, and makes only 1 query.

- ElGamal scheme in the multi-user setting almost as secure as it is in the single user setting.