# Public-key Cryptography I

CPA, CCA definitions,
hybrid models (KEM/DEM)

# Basic Definition

- A public key encryption scheme consists of 3 poly-time algorithms:

  - (PK,SK) <— KeyGen ($1^n$): randomized algorithm
  - C <— Encrypt (PK,M): randomized
  - M <— Decrypt (PK,SK,C): deterministic

- We'll use $E_{PK}(M)$, and $D_{SK}(C)$
- It is required that $D_{SK}(E_{PK}(M))$ —> M, except with negl. probability in n

# IND-CPA Game

- Natural analogue of IND-CPA for shared-key crypto
- Played between adversary, A, and challenger

- Game:
  - Challenger runs KeyGen ($1^n$) —> (PK,SK)
  - A given PK, outputs $m_0, m_1$
  - Challenger does $E_{PK}(m_b)$ —> C, C given to A
  - A outputs b′. If b′=b, A wins

- A public-key encryption scheme is IND-CPA secure if for all PPT adversaries, there is a negl. function, s.t.,

$$\Pr[A(PK,n) = b'; b=b'] \leq 1/2 + \mathrm{negl}(n)$$

# Deterministic PKE

- Deterministic PKE is CPA-insecure
- Similar to shared-key setting

- Grading example
  - Grades $\in$ {A,B,C,D,F}, PK of instructor known
  - Adversary just does $C_A = E_{PK}(A)$, $C_B = E_{PK}(B)$, … compare with any given encrypted grade

- Duh? Was used from mid-1970s-1984

# IND-CCA Game

- Played between adversary, A, and challenger
- Game:
  - Challenger runs KeyGen $(1^n)$ —> (PK,SK)
  - A given (PK, *decryption oracle* $Dec_{SK}(\bullet)$), outputs $m_0, m_1$
  - Challenger does $E_{PK}(m_b)$ —> C, C given to A
  - A queries $Dec_{SK}(\bullet)$, except A cannot ask decryption of C
  - A outputs b′. If b′=b, A wins

# IND-CCA Game

- A public-key encryption scheme is IND-CCA secure if for all PPT adversaries, there is a negl. function, s.t.,

$$\Pr[A(PK,n) = b'; b=b'] \leq 1/2 + \mathrm{negl}(n)$$

- "Oracle"…?
  - Just a black-box functionality[1]
  - Used to provide access to restricted functionalities to A
  - Here, parametrized with SK



1: More precisely, a mathematical abstraction that models a black-box functionality

# CPA/CCA for Multiple Encryptions

- Examines consequences of using same PK for encrypting multiple messages
- Turns out, any CPA/CCA-secure PKE scheme, *automatically* also has CPA/CCA-security for multiple messages![1]
- Single-message CPA/CCA-security implies multi-message CPA/CCA-security
- Very useful result! Do proofs in simple case, strong result follows…

1: Due to Bellare et al., Crypto '98

# Hybrid Encryption

- Basic idea: setup a shared key, K, using PKE, thereafter use K for all encryption
- Motivation: PKC too slow,
- Used extensively in practice
- Functionality of PKC + efficiency of SKC
- Hybrid algorithms: Key Encapsulation Mechanism (KEM), Data Encapsulation Mechanism (DEM) schemes

# Key Encapsulation Mechanism (KEM)

- A KEM scheme consists of 3 poly-time algorithms
  - (PK,SK) <— KeyGen ($1^n$): randomized algorithm
  - (C,K) <— Encapsulate (PK,$1^n$,$1^k$): randomized, |K|=k
  - {K,⊥} <— Decapsulate (PK,SK,C): deterministic
- It is required that $\text{Decapsulate}_{SK}$(C) —> K, except with negl. probability in n
- DEM – just regular shared-key encryption scheme (E,D,K)

# KEM/DEM Paradigm

- Let $\Pi$ be a KEM scheme, and $\Pi'$ be a DEM scheme. Then a hybrid encryption scheme $\Pi^{hy}$ is defined as:

- (PK,SK) <— KeyGen($1^n$): randomized
- (C,C′) <— Encrypt (PK, M): randomized
    - do (C,K) <— Encapsulate($1^n$,$1^k$)
    - do C′ <— $E_K$(M)
    - return (C,C′)
- M <— Decrypt(C,C′): deterministic
    - do K <— Decapsulate(C)
    - return M <— $D_K$(C′)