UNIVERSITY OF DELAWARE

CYBERSECURITY

Applied Cryptography
CPEG 472/672
Lecture 1B

Instructor: Nektarios Tsoutsos

Encryption security

- What is the definition of security?
  - ”nothing can be learned” even given many ptxt-ctxt pairs
- Attack model
  - Assumptions about attacker powers
- Security goals
  - What is considered a successful attack

Black box models

- Ciphertext-only attack (COA)
  - Passively observe ctxts, no Enc/Dec queries
- Known-plaintext attack (KPA)
  - Known random ptxt/ctxt pairs, passive
- Chosen-plaintext attack (CPA)
  - Active enc queries for selected ptxts
- Chosen-ciphertext attack (CCA)
  - Active enc & dec of chosen ptxts/ctxts

Gray box models

- Attacker knows cipher implementation
  - More realistic for IoT, embedded systems
- Side channel attacks
  - Non-invasive
  - Measure implementation parameters
- Invasive attacks
  - Fault Injection attacks

Security goals

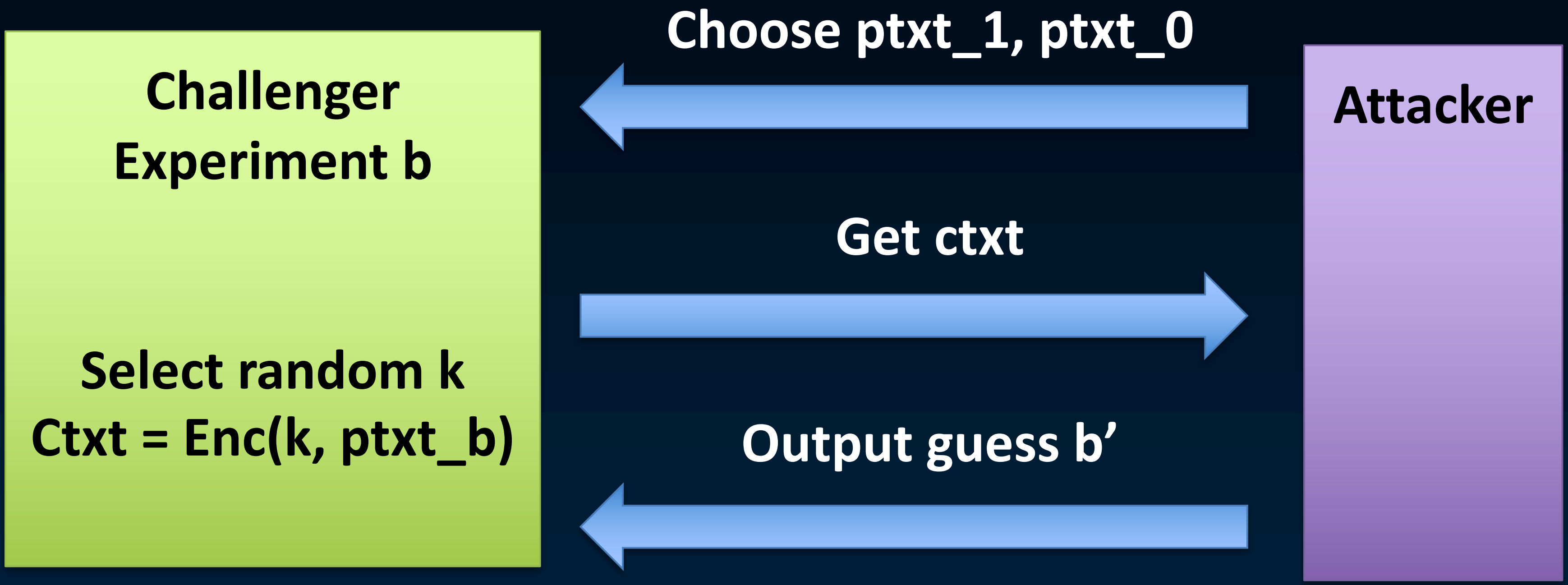
- Indistinguishability (IND)
  - Attackers cannot distinguish ctxt from random strings
- Non-malleability (NM)
  - Attackers cannot create ctxt2 from ctxt1 where ptxt2 has meaningful a relationship to ptxt1

Security notions (GOAL-MODEL)

- IND-CPA
  - Also known as semantic security
  - Can be achieved using randomized enc
    - Ctxt = Enc(K, random_num, ptxt)
    - Ctxts are longer than ptxts
- Notion relations
  - IND-CCA => IND-CPA, NM-CCA => NM-CPA
  - IND-CPA DOES NOT imply NM-CPA
  - NM-CPA => IND-CPA
  - IND-CCA <=> NM-CCA (equivalent notions)

The IND-CPA challenge

- ptxt_1 and ptxt_0 have the same length



- We want the Probability of b’==b (i.e., correctly predicting b) to be 0.5

A semantically secure cipher

- Use a deterministic random bit generator
- Cipher inputs
  - Key k, random string R, plaintext ptxt
- Cipher outputs
  - Ciphertext ctxt, copy of R
- (ctxt, R) = (DRBG(k || R) XOR ptxt , R)
  - This offers IND-CPA but not NM-CPA
  - Ctxt XOR 1 is the encryption of ptxt XOR 1

Asymmetric encryption

- Encryption inputs
  - Public key PUB, plaintext ptxt
- Decryption inputs
  - Private/secret key PRI, ciphertext ctxt
- What are the attack models in this case?
- As before, but default is CPA
  - Attacker knows the public key
  - Attacker can encrypt any ptxt at will

Reading for next lecture

- Aumasson: Chapter 2