

Public Key Encryption

Rohit Musti

CUNY - Hunter College

March 23, 2022

Table of Contents

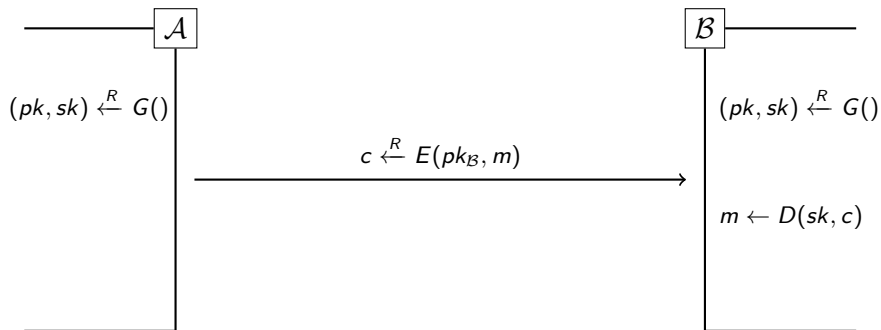
- 1 Overview
- 2 Semantic Security
- 3 Chosen Plaintext Attack Security
- 4 Chosen Ciphertext Attack Security

1 Overview

Recap

- Last lecture we discussed an example of how to exchange secret keys "in the clear"
- This allows us to re-use our symmetric key cryptography protocols to exchange information in the public!
- We also discussed two real-world examples of key exchange (Diffie-Hellman and RSA)
- In the lecture prior to that we introduced the notion of asymmetric encryption, outlined its basics. Today we will dive into its security!

Public Key Encryption Overview



Benefits

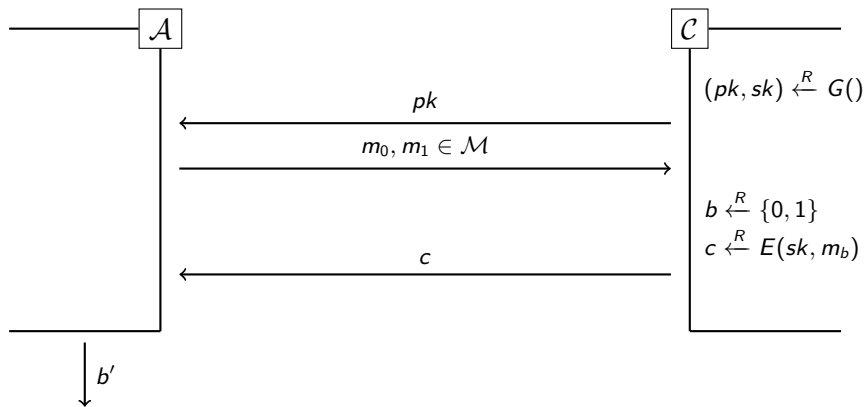
- 1 Public key encryption is often referred to as *assymmetric encryption* because the encryptor and decryptor use different keys (unlike *symmetric encryption* which uses the same keys)
- 2 After the public key is securely obtained, there is only one interaction to send a message!
- 3 We can re-use the public key many times
- 4 Anyone can post their public key for everyone else to see (no key exchange required), this means that the secret keys must not be derivable from public keys

2 Semantic Security

Review of Semantic Security

- The intuition of semantic security is that the probability a computationally bounded adversary can learn anything about a message from its ciphertext is negligible
- Semantic security guarantees that a message cannot be recovered from a ciphertext

Public Key Semantic Security Attack Game



if $b' = b$, then the adversary wins

Semantic Security Randomization

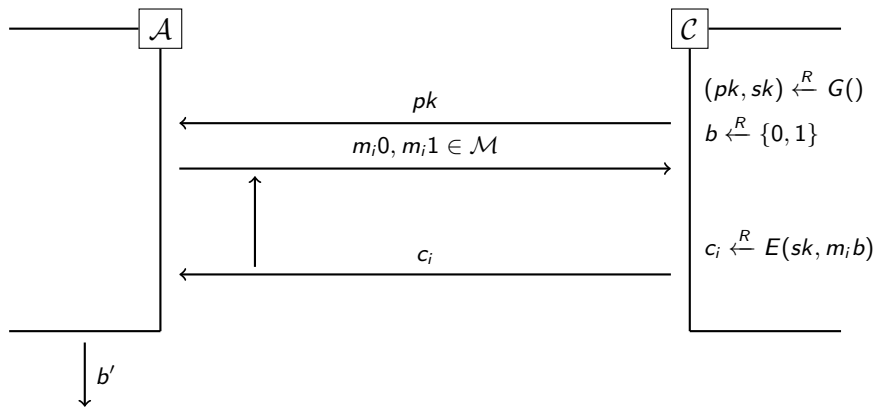
- For public key semantic security, the encryption function must be random. Can we think of an attack???
- Future Homework Assignment!

3 Chosen Plaintext Attack Security

Public Key CPA Security

- Semantic security does not imply CPA security in symmetric key cryptography schemes
- The intuition behind this is that in a symmetric key security setting, the attacker cannot encrypt their own messages into their own cipher texts (because they don't have access to the key)
- In a public key setting, the adversary doesn't even need to interact with the challenger to get cipher texts

Public Key CPA Attack Game



if $b' = b$, then the adversary wins

4 Chosen Ciphertext Attack Security

CCA Overview