Week 5

Lecture 1

Part 1: Public Key Cryptography: RSA Digital Signature
Part II: Security of RSA

Lecture 2

Revisiting Modes of Encryption and any left-over mathematics.

Workshop 3: Workshop based on Lectures in Week5

Quiz 5

Public Key Cryptography: Diffie-Hellman and RSA

Lecture 1

Part I

- 1.1 RSA Digital Signature
  - Digital Signature Introduction.
  - Different Versions RSA Signatures.
  - Signature Algorithm in Practice

- 1.2 Mathematical Attacks
  - Security of RSA
  - Elementary Attacks
  - Status of Factorization problem

Part II Security of RSA

- 1.3 Security Notions and Attack Models
  - Security Notions
  - CCA Attack
  - Timing Attacks

1.3 Security Notions and Attack Models

COMP90043

Lecture 1

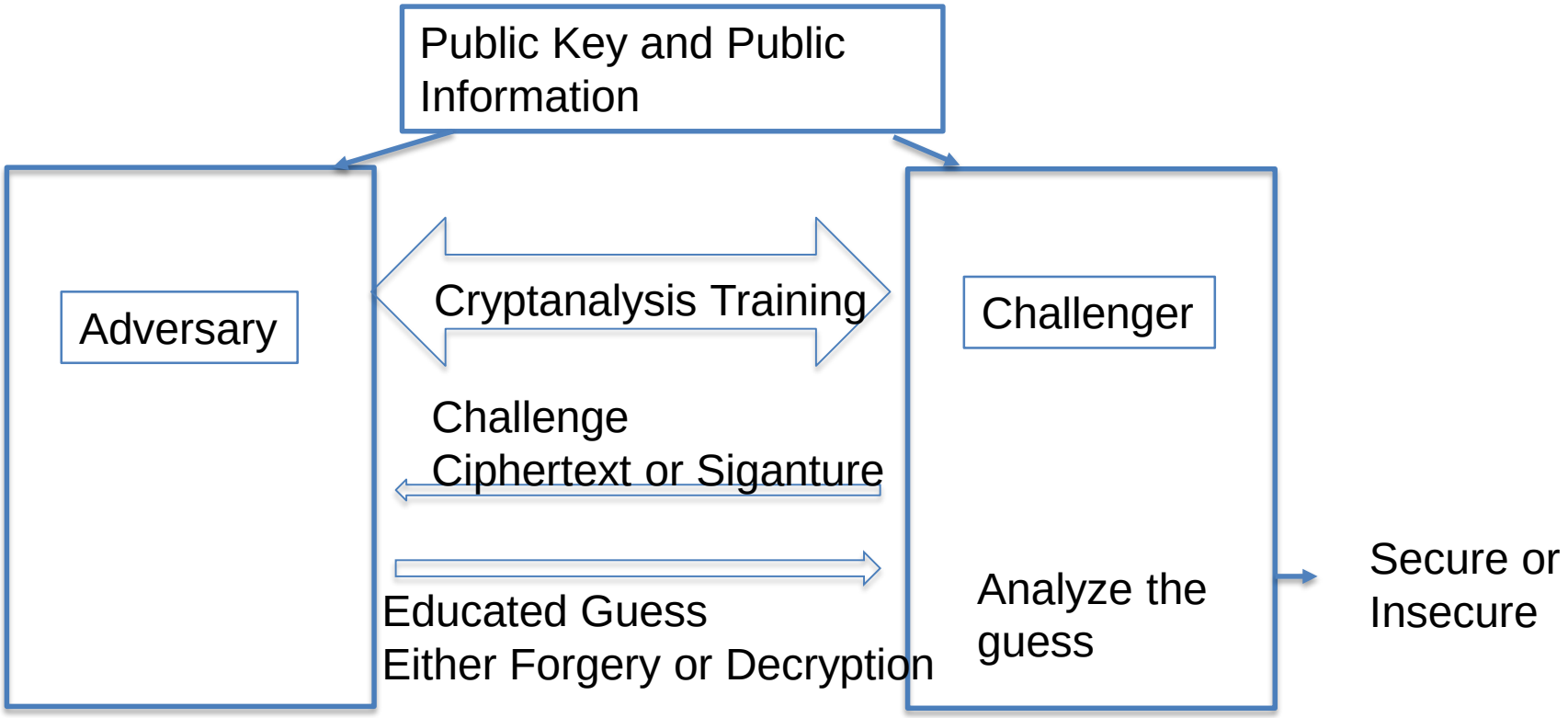
Udaya Parampalli

Security Notions

- We introduced security notions for public key cryptography in the previous weeks.
  - The security of a cryptosystem is defined with respect to the attacks it can withstand.
  - The attacker will not be given private or secret information of the cryptographic key whose public cryptosystem he is attacking.
- There are three types of active attacks:
  - **Chosen-plaintext attack(CPA)**
    - Encryption box is available to the attacker before the attack.
    - Here the attacker can obtain cipher texts corresponding any chosen plain texts. The goal is to weaken the crypto system with the obtained plaintext-ciphertext pairs
    - In Public Key Cryptography, attacker can create as many public keys as he can to study its security. Interesting attacks are in fact with breaking decryption, i.e CCA attacks:
  - **Chosen-ciphertext attack(CCA)**
    - Decryption box is available to the attacker before the attack.
  - **Adaptive Chosen-ciphertext attack(CCA2)**
    - Decryption box is available to the attacker except for the challenged ciphertext.
    - Here attacker can obtain plaintexts corresponding any chosen ciphertexts. This means the attacker gets decryption assistance for any chosen ciphertext. The goal for the attacker is to obtain any part of the plaintext after the decryption assistance is terminated.

Attack Model

- We create a game involving Challenger and Adversary.



Justification for the Attack Model

- The framework need to capture the practical realities when analysing the strength of cryptosystems.
- In reality, sometime encryption box or decryption box are available to practical adversaries.
- The analysis will help to evaluate the security of the system.
- Main goal is capture all types of practical attacks, which is not easy in general.
- The textbook RSA is naturally not suited work in this framework.
- In the next slide, we show how RSA is vulnerable to CCA.

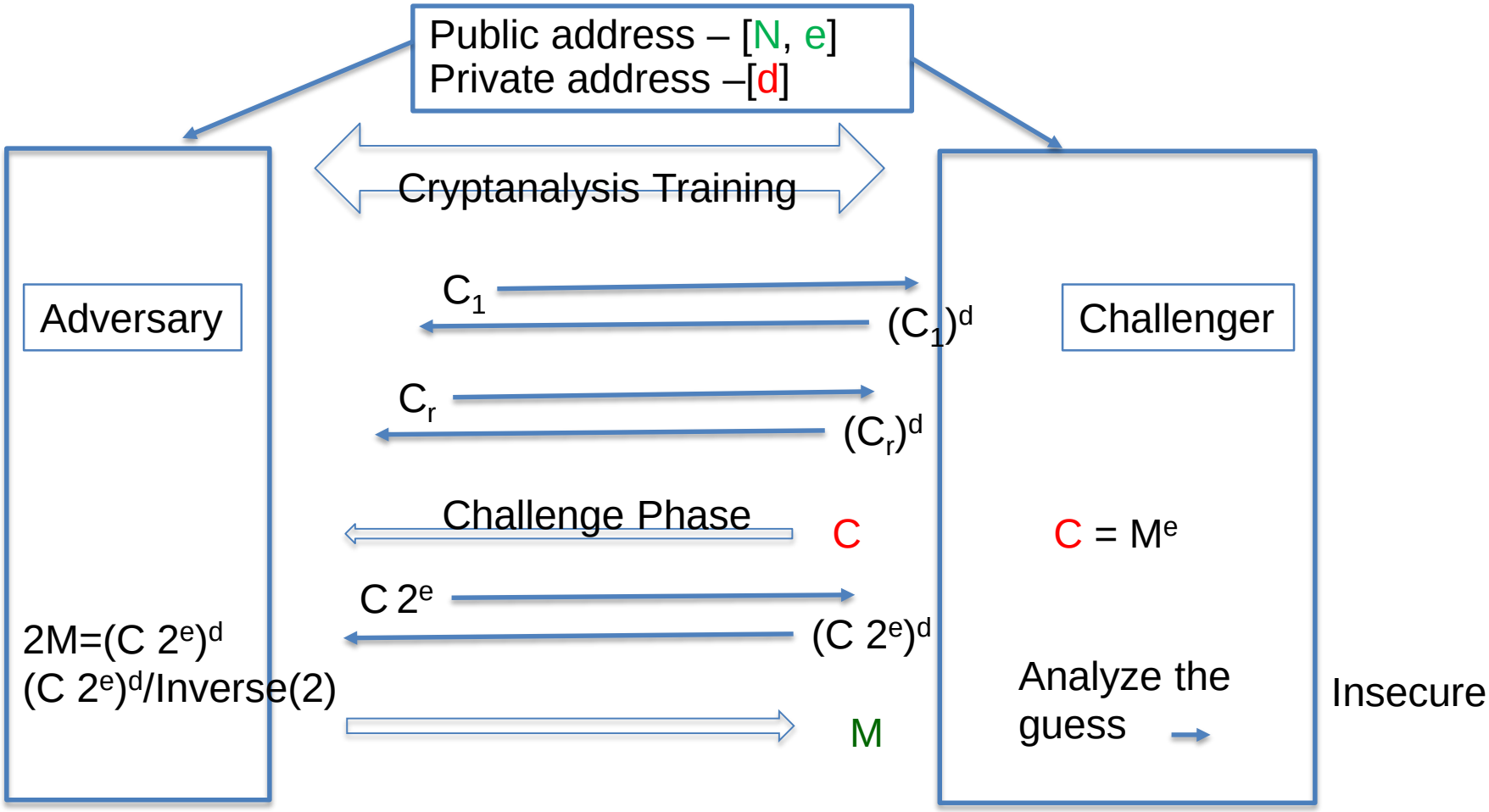
CCA Security

- The basic RSA algorithm is vulnerable to a chosen ciphertex tattack (CCA).
- In this scenario, the adversary gets decryption of a number of ciphertexts of his choice.
- Adversary will then be given a challenge cipher text for which he has to produce the decryption (without having access to the private key).
- This is because of the multiplicative Property of the RSA Algorithm:

$$(M_1 \times M_2)^e = M_1^e \times M_2^e = (M_1 \times M_2)^e$$

$$(C_1 \times C_2)^d = C_1^d \times C_2^d = (C_1 \times C_2)^d$$

Attack



Adversary can choose any value b (instead of s) to blind the ciphertext
But (b, n) =1

Practical RSA: Use RSA with OAEP

- To overcome the previous attack, you need somehow break the multiplicative property of the scheme.
- In practice message is introduced with a specific format, which removes the multiplicative property.
- OAEP is one such formatting method. Please follow Fig 9.10 of the textbook

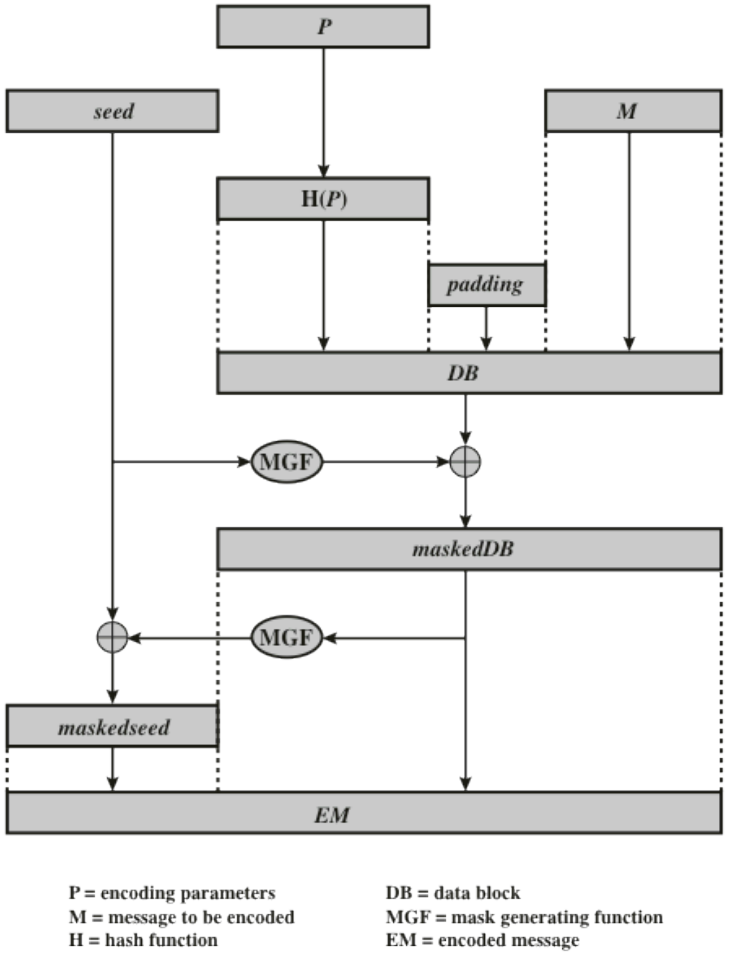


Figure 9.10 Encryption Using Optimal Asymmetric Encryption Padding (OAEP)

Timing Attacks

- Timing attacks are slightly different to the previous attacks. There is a surprise element to it.
- Here the attacker will observe the behaviour of the Cryptographic algorithms to different inputs and use the experience to break the secret directly.
- It can be devastating especially because adversary only needs ciphertexts.
- The attack is applicable wide range of cryptographic algorithms.
- If you observe variability in any aspects of the crypto algorithm, you may be able to convert into an attack. The generalizations of this attack include power analysis attack and fault based attack. The later, a certain faults are introduced deliberately and attacker studies the algorithm.
- Please refer Chapter 9 for more details.

Counter measures for Timing attacks

- **Constant time:** One way is to make sure that your algorithm takes a constant time for all inputs. This approach requires you to estimate the longest delay in advance and use appropriate idle time when results take less than the worst case time. However, this method may still leak power profile. In general performance decreases in efficiency.

- **Random delay**: You will add a random delay to algorithm execution to ensures that the relationship between key and the execution time is uncorrelated.

- **Blinding**: You can use the blinding technique introduced earlier. With this, the algorithm takes a random amount time and assures that the relationship between key and the execution time is uncorrelated.

Week 5

Lecture 1

Part 1: Public Key Cryptography: RSA Digital Signature
Part II: Security of RSA

Lecture 2

Revisiting Modes of Encryption and any left-over mathematics.

Workshop 3: Workshop based on Lectures in Week5

Quiz 5