MAS 433: Cryptography

Lecture 16
Public Key Encryption
Part 3: OAEP

Wu Hongjun

Lecture Outline

- Classical ciphers
- Symmetric key encryption
- Hash function and Message Authentication Code
- Public key encryption
  - RSA
    - Specification
    - Implementation
    - Security
  - ElGamal
  - **Message padding (OAEP)**
- Digital signature
- Key establishment and management
- Introduction to other cryptographic topics

Recommended Reading

- CTP: Section 4.9
- Wikipedia
  - Optimal asymmetric encryption padding
    - http://en.wikipedia.org/wiki/Optimal_asymmetric_encryption_padding
  - PKCS
    - http://en.wikipedia.org/wiki/PKCS

"Textbook" RSA Encryption

- RSA Encryption

  $$c = m^e \bmod n \qquad \text{(plaintext } m\text{: } 0 < m < \text{n)}$$

- Risks
  - Property:

    $$\text{If } m = \prod_{i=1}^{t} m_i \text{ , then } c = \prod_{i=1}^{t} c_i \bmod n \text{ , where } c_i = m_i^e \bmod n$$

  - Encryption algorithm is **deterministic** & public
    - The same plaintext is always encrypted to the same ciphertext
      - If the message size is small, …
      - If the public key size is small, ….

Padding RSA

- **Never use the "textbook" RSA in practice**

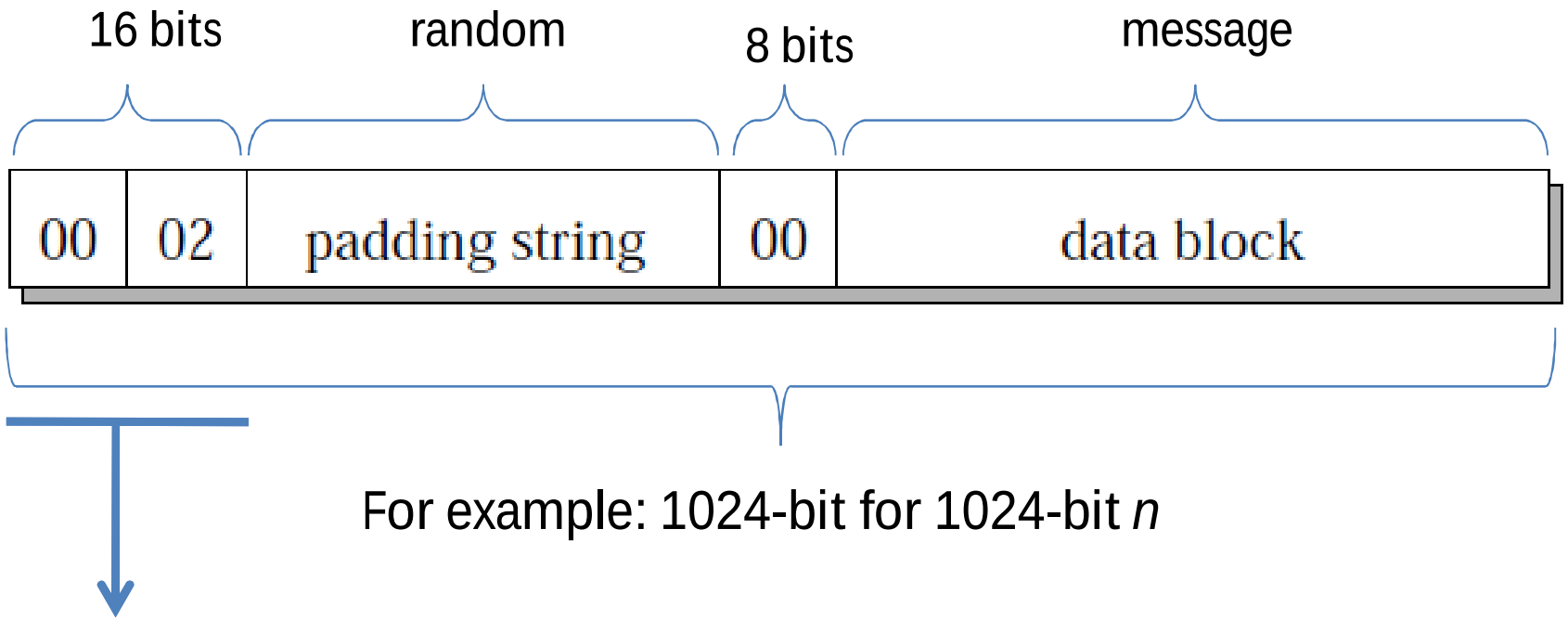
- Padding is necessary
  - Pad the message to large size
  - Introduce randomness to the encryption algorithm
    - We cannot make the encryption algorithm secret
    - We cannot eliminate the multiplicative property between the plaintext & ciphertext

Insecure Padding in PKCS#1 v1

- What is PKCS#1 ?
  - PKCS
    - Public-Key Cryptography Standards
    - published by RSA Laboratories
  - PKCS#1
    - RSA Cryptography Standard
    - definitions of and recommendations for implementing the RSA algorithm
    - Current version: 2.1 (2002)
      - also in RFC 3447 (2003)

Insecure Padding in PKCS#1 v1

- Padding in PKCS#1 v1.5



It indicates Mode 2 (encryption)

After decrypting a ciphertext, it is checked whether the value of the first two bytes is 0x02

Insecure Padding in PKCS#1 v1

- Attack on PKCS#1 v1 (1998)
  (not required for exam)
  - An attacker tries to test if the MSBs of plaintext is 0x02
    - Pick a random r, compute $C' = r^e \cdot C \bmod n$
    - Send C' to web server and check the response
    - If there is no error message, it means that the first two bytes of $(r \cdot m_{pad}) \bmod n$ is 0x02
  - The plaintext can be gradually recovered with about 2^{20} chosen ciphertexts

Insecure Padding in PKCS#1 v1

- Consequence
  - PKCS#1 is used in SSL3.0
    - SSL3.0 widely used in web servers and browsers in 1998

Strong Padding: OAEP in PKCS#1 v2

- OAEP (1994)
  - Optimal asymmetric encryption padding
- PKCS#1 v2.0 (1998)
  - Use OAEP to resist the chosen ciphertext attack on PKCS#1 v1

Strong Padding: OAEP in PKCS#1 v2

- OAEP

(the specification here is slightly different from the RFC)

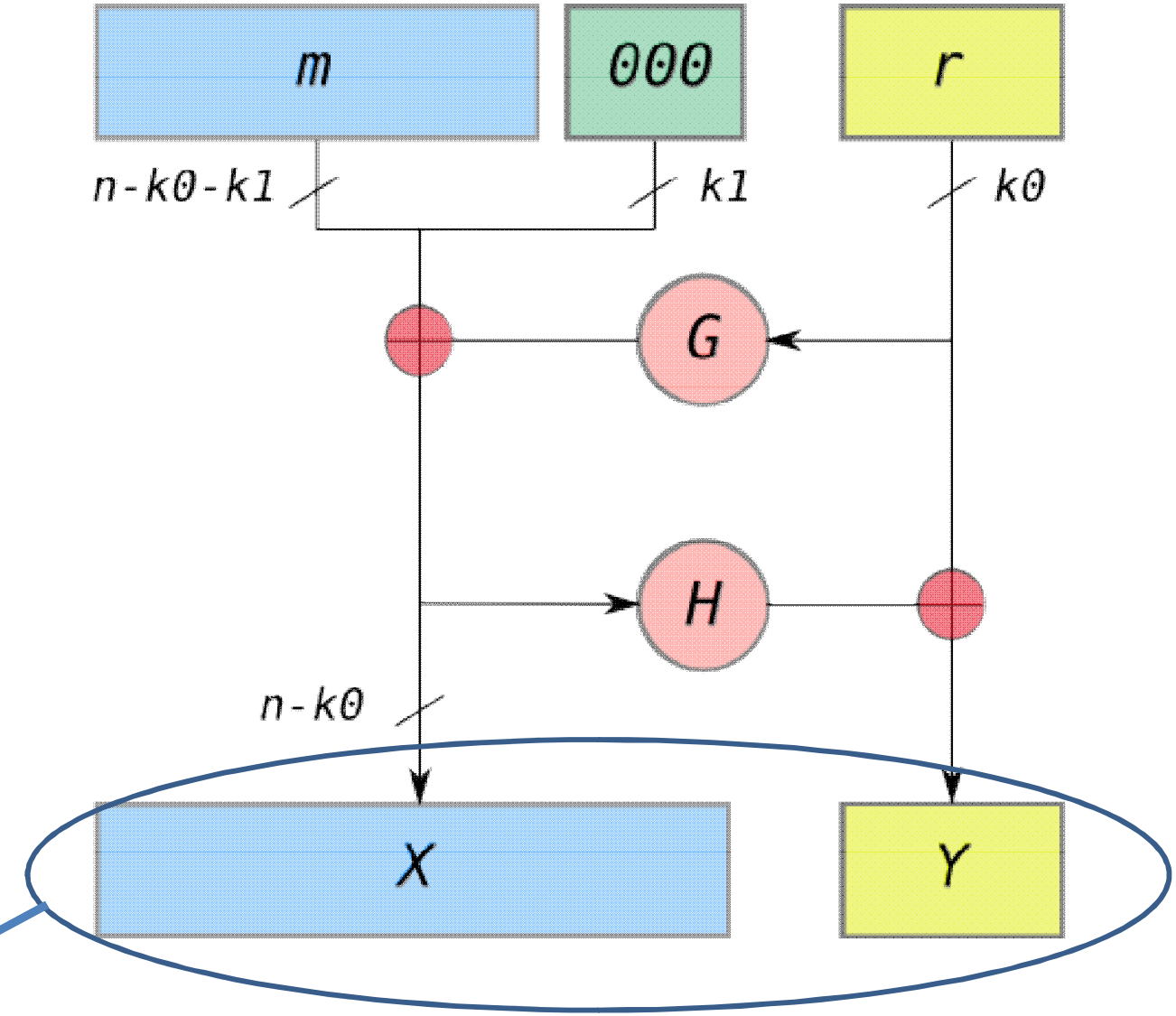
n: the number of bits in the RSA modulus.

k_0 and k_1: integers fixed by the protocol

m: plaintext message, $(n - k_0 - k_1)$-bit string

G and *H:* *"random"* functions fixed by the protocol

The padded message to be encrypted



Strong Padding: OAEP in PKCS#1 v2

- Security of OAEP
  - "Provably" secure, 1994
    - Complicated security proof
    - Get standardized for its security proof
  - OAEP's security proof is found to be incorrect, 2001
    - But OAEP is still strong enough for applications

Summary

- "Textbook" RSA encryption
  - Deterministic & public encryption algorithm
  - Do not use it practice
- Padding is needed
  - Use the strong OAEP
    - Introduce the randomness into the encryption process