PKCS #1

Hyoungshick Kim

Department of Software

College of Software

Sungkyunkwan University

PKCS #1 v1.5

- Standard issued by RSA labs in 1993
- Idea: Add random padding
  - To encrypt m, choose random r
  - $C = [(r|m)^e \bmod N]$
- Issues:
  - No proof of CPA-security (unless m is very short)
  - Chosen-plaintext attacks are known if r is too short
  - Chosen-ciphertext attacks are known

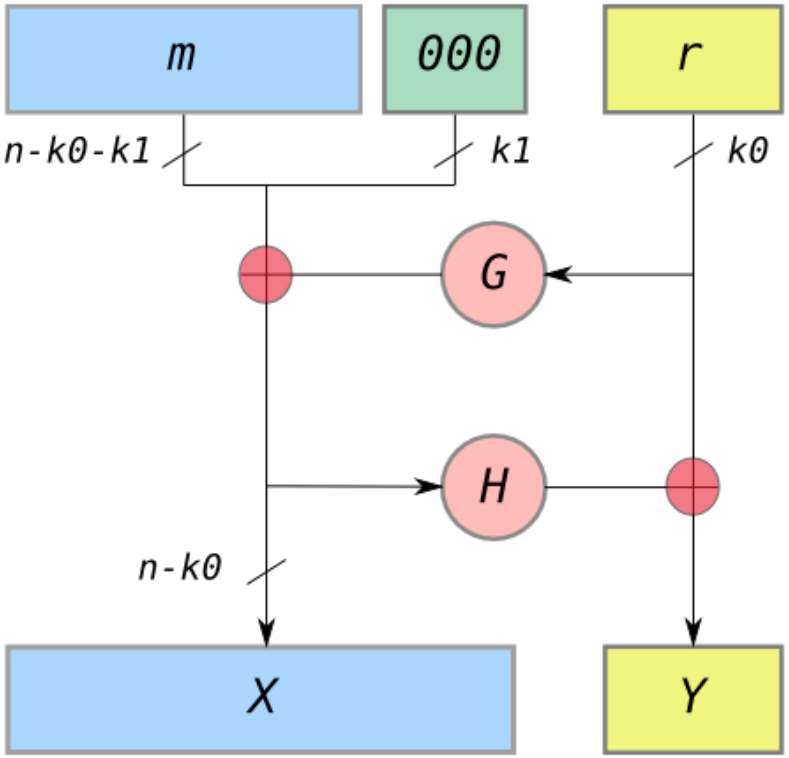
PKCS #1 v2.0

- Optimal asymmetric encryption padding (OAEP) applied to message first
- This padding introduces redundancy, so that not every $c \in Z^*_n$ is a valid ciphertext
  - Need to check for proper format upon decryption
  - Return error if not properly formatted
- RSA-OAEP can be proven CCA-secure under the RSA assumption, if G and H are modeled as random oracles

OAEP

- By Bellare & Rogaway, 1994; in RFC 2437

$C = [(x|y)^e \bmod N]$



OAEP looks like a kind of Feistel network.

RSA-OAEP operations

- Encryption with the plaintext m
  1. $x \leftarrow m \mid 0^{k_1} \oplus G(r)$
  2. $y \leftarrow H(x) \oplus r$
  3. $C = [(x|y)^e \bmod N]$

- Decryption with the ciphertext c
  1. $x|y \leftarrow c^d \pmod N$ satisfying $|x| = n-k_0$, $|y| = k_0$
  2. $u \leftarrow y \oplus H(x)$; $v \leftarrow x \oplus G(u)$ // u = r
  3. Output m if $v = m \mid 0^{k_1}$, else reject.

Questions?


Sungkyunkwan
Campus
Social
Graduate
Professors
English
Confucian
campus
Zone
Sciences
University
Global
Education
Seoul
Natural
Suwon
Korean
School
university
established
edit
also
Humanities
Science
schools
Administration
ASLE-Korea
Academic
Advanced
constructed
Building
Engineering
located
Joseon
Anniversary
Institute
now
two
Hall
Course
lecturers