Lecture 14
Outline

CCA attacks

CCA security
Textbook RSA Enc \[ (M) = M^e \mod N \]

Dec \[ d, N (ct) = ct^d \mod N \]

\[ = (M^e)^d \mod N \]

\[ = M^{(k \cdot \phi(N)+1)} \mod N \]

\[ = M^{\phi(N)} \mod N \]

\[ = (M^{\phi(N)})^k \cdot M \mod N \]

\[ = \left( M^{\phi(N)} \right)^k \cdot M \mod N \]

\[ \text{(Legendre's Thm)} \]

\[ M \ll N. \]
PKCS1 used in HTTPS:

\[ \Rightarrow \text{attacker can test if 16 MSBs of plaintext } = '02' \]

Chosen-ciphertext attack: to decrypt a given ciphertext \( C \) do:

- Choose \( r \in \mathbb{Z}_N \). Compute \( c' \leftarrow r^e \cdot c = (r \cdot \text{PKCS1}(m))^e \)
- Send \( c' \) to web server and use response
Baby Bleichenbacher

Suppose N is $N = 2^n$ (an invalid RSA modulus). Then:

- Sending $c$ reveals $\text{msb}(x)$
- Sending $2^e \cdot c = (2x)^e$ in $\mathbb{Z}_N$ reveals $\text{msb}(2x \mod N) = \text{msb}_2(x)$
- Sending $4^e \cdot c = (4x)^e$ in $\mathbb{Z}_N$ reveals $\text{msb}(4x \mod N) = \text{msb}_3(x)$
- ... and so on to reveal all of $x$

Given $c = \text{Enc}(M)$

- $2^e c = \text{Enc}(2M)$
- $4^e c = \text{Enc}(4M)$

$c' = c \cdot r^e \mod N = \text{Enc}(M \cdot r)$
```
0/1

Server

\[ c' \]

\[ c \]

\[ (2^{128})^e \cdot c \mod N \]

\[ 00 \text{ msg} \]

\[ 11 \ldots 1 \]

\[ 0 \ldots 0.1 \]

\[ n \]

\[ n-1 \]

\[ n-3 \]

\[ 00100 \ldots \]

divide by 2.

multiply by 2.
```
Chosen Ciphertext (CCA) security for Public Key Encryption

• H: Truly random function

• “Observable”
  To obtain $H(q)$, A must have computed $H$ on $q$.

• “Programmable”
**PKCS1 v2.0: OAEP**

New preprocessing function: OAEP  

Thm [FOPS’01]: RSA is a trap-door permutation \( \Rightarrow \)  
RSA-OAEP is CCA secure when \( H, G \) are random oracles

in practice: use SHA-256 for H and G
What is a random oracle?

- H: Truly random function
- "Observable"
- "Programmable"
The factoring problem

Gauss (1805): "The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic."

Best known alg. (NFS): run time $\exp(\tilde{O}(\sqrt[3]{n}))$ for n-bit integer

Current world record: RSA-768 (232 digits)
• Work: two years on hundreds of machines
• Factoring a 1024-bit integer: about 1000 times harder
  ⇒ likely possible this decade
Summary

• Key concepts in number theory

• Hardness of discrete logarithm, factoring

• Diffie-Hellman key exchange from hardness of DDH

• Public key encryption => shared key derivation (called key exchange)