

The background of the slide is an abstract painting. It features broad, textured brushstrokes in various shades of green, ranging from light lime to deep forest green, and various shades of blue, from pale sky blue to deep navy. The colors are layered and blended, creating a sense of depth and movement. The texture of the paint is visible, with some areas appearing more saturated than others.

Lecture 14

Scribe : Eshrit

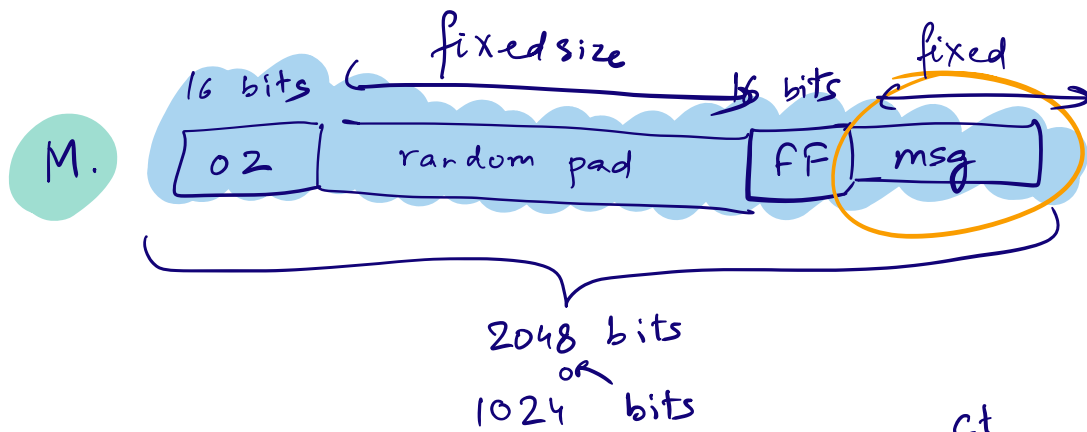
Outline



CCA attacks



CCA security



Textbook - RSA - $\text{Enc}_{e,N}(M) = M^e \text{ mod } N$

ct

$$\begin{aligned} \text{Dec}_{d,N}(ct) &= ct^d \text{ mod } N \\ &= (M^e)^d \text{ mod } N \\ &= M^{(k\phi(N)+1)} \text{ mod } N \end{aligned}$$

[Because $e \cdot d = 1 \text{ mod } \phi(N)$]

$$= \left(M^{\phi(N)} \right)^k \cdot M \text{ mod } N$$

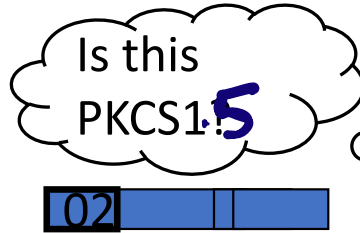
(Fermat's Thm)

$$M < N$$

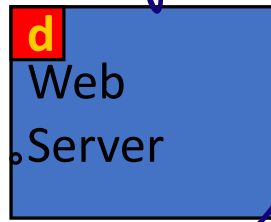


CCA Attack on PKCS1 v1.5 (Bleichenbacher 1998)

PKCS1 used in HTTPS:



RSA
decryption key



yes: continue
no: error



c = ciphertext

⇒ attacker can test if 16 MSBs of plaintext = '02'

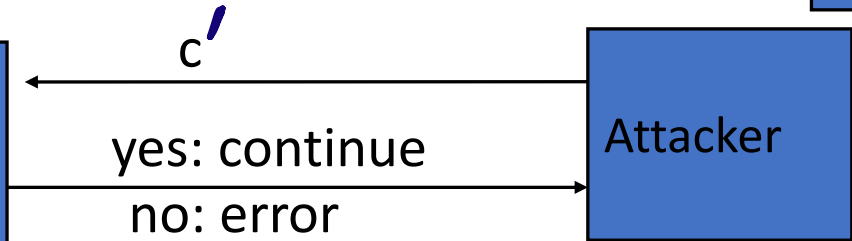
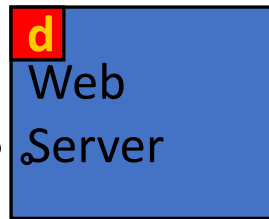
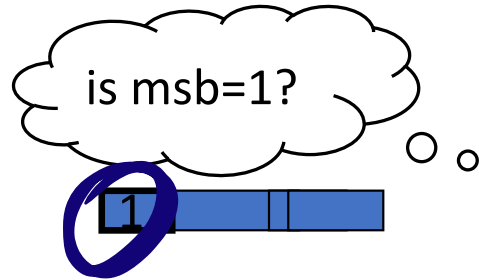
Does $(c')^d$ have msb = 02

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

compute $x \leftarrow c^d$ in Z_N



$$c = M^e \bmod N$$

$$c' = c \cdot r^e \bmod N = (M \cdot r)^e \bmod N = \text{Enc}(M \cdot r)$$

$c =$ ciphertext

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 Z_N
- Sending $4^e \cdot c = (4x)^e$ in Z_N
- ... and so on to reveal all of x

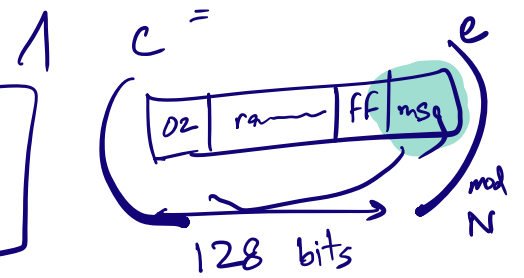
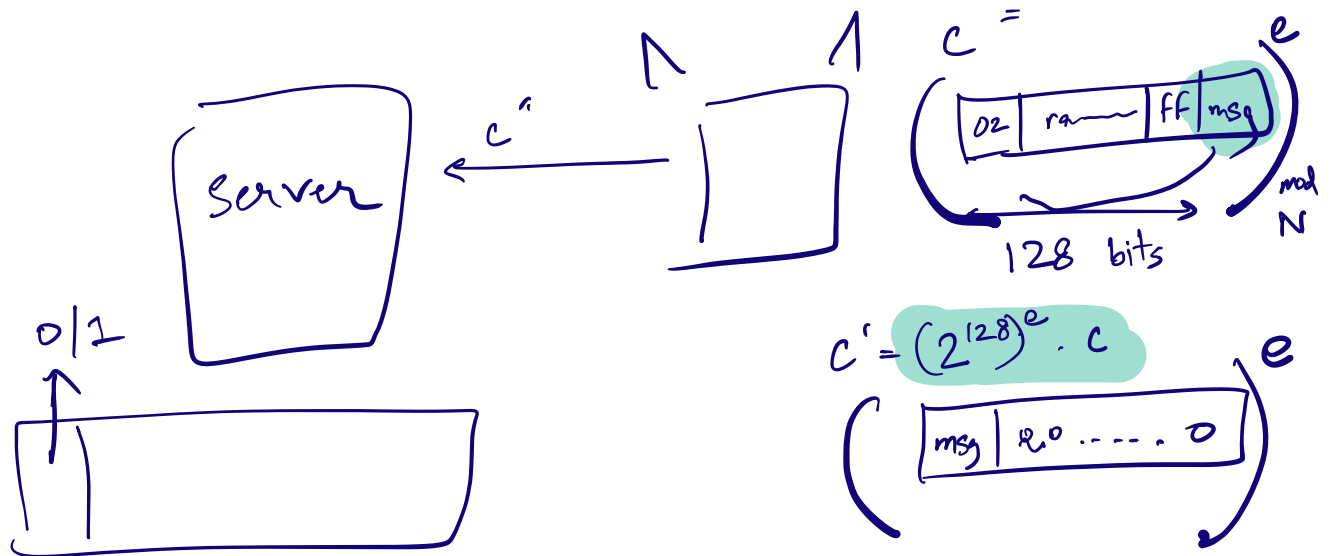
reveals $\text{msb}(2x \bmod N) = \text{msb}_2(x)$

reveals $\text{msb}(4x \bmod N) = \text{msb}_3(x)$

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

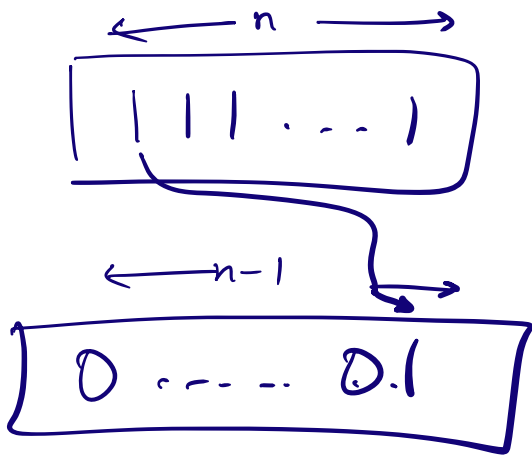
$$2^e c = \text{Enc}(2M)$$

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

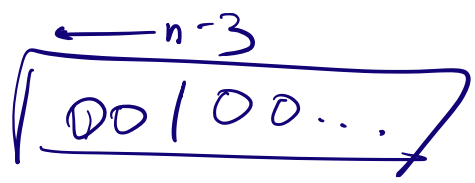


$$c^r = (2^{128})^e \cdot c \pmod{N}$$

Diagram illustrating the encryption process: $c^r = (2^{128})^e \cdot c \pmod{N}$. The message 'msg' is padded with zeros to 128 bits, then encrypted with exponent e modulo N to produce c .



divide by 2.



multiply by 2

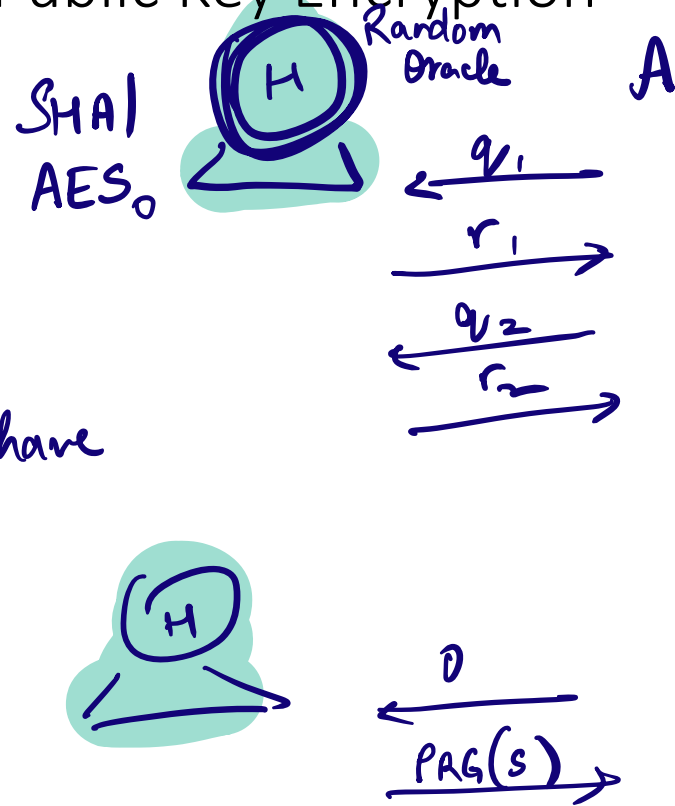
RANDOM ORACLE

Chosen Ciphertext (CCA) security for Public Key Encryption

- H: Truly random function

- "Observable" (PPT)
To obtain $H(q)$, A must have
computed H on q .

- "Programmable"

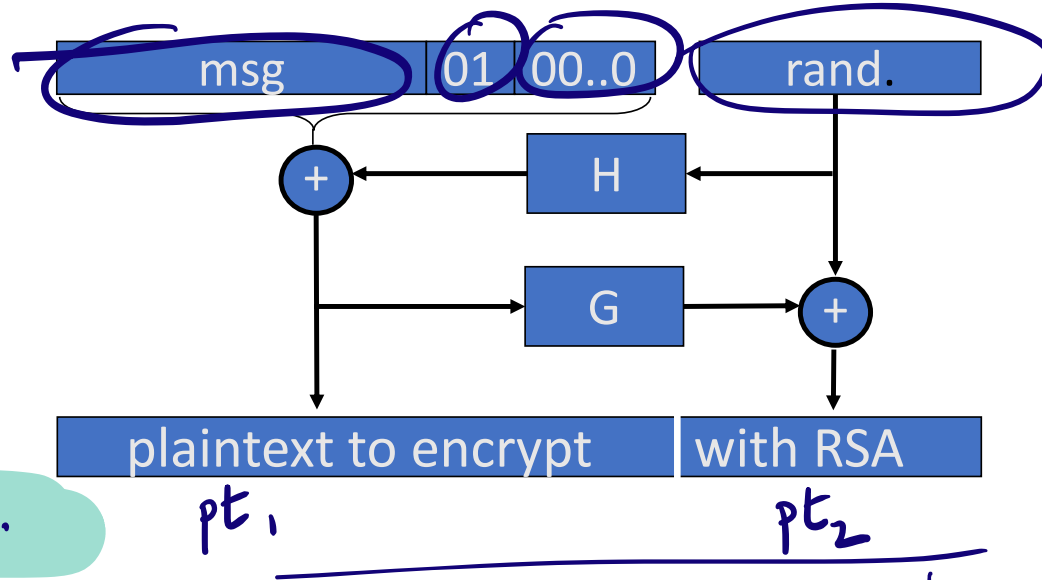


PKCS1 v2.0: OAEP

Bellare - Rogaway.

New preprocessing function: OAEP [BR94]

check pad
on decryption.
reject CT if invalid.



$$pt_1 = (msg, 01, 00..0) \oplus H(rand)$$

$$pt_2 = G(pt_1) \oplus rand.$$

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”

Handwritten mathematical formulas illustrating a random oracle construction, with red and blue annotations:

$$pt_1, pt_2$$
$$rand = G(pt_1) \oplus pt_2$$
$$(msg, 01, 0...0) = pt_1 \oplus H(rand)$$

The annotations include a red box around pt_1, pt_2 , a red circle around $G(pt_1)$, a red circle around $H(rand)$, and a blue box around the message input $(msg, 01, 0...0)$ in the third equation. A red arrow points from the $G(pt_1)$ term in the second equation to the $H(rand)$ term in the third equation.

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 \Rightarrow shared key derivation (called key exchange)