Introduction to Modern Cryptography

10th lecture:
RSA encryption
CCA security
last time:
• Definition PubK
• eav => CPA
• multi-message security
• hybrid encryption
• El Gamal

10th lecture (today):
• RSA Encryption
• CCA security
Taher Elgamal
*1955

- 1977: BSc from Cairo University
- 1984: PhD from Stanford
- 1996: “Father of SSL” as Chief Scientist of Netscape
- CTO of various companies

fun fact: “I read number theory books for fun!”
Ron Rivest
*1947

Adi Shamir
*1952

Leonard Adleman
*1945

• as MIT students
• in 2003
Insecurity of Textbook RSA

• Textbook RSA is deterministic, thus not even eavesdropper secure!

• **weak guarantee** under RSA assumption: no PPT adv can recover from the ciphertext the entire message $m$ if chosen at random

• If $N$ can be factored $\Rightarrow$ RSA problem is easy

• but we **do not know** if RSA problem is as hard as factoring
Padded RSA

- For $\ell(n) = 2n - O(\log n)$, $r$ can be guessed in polynomial time, not CPA secure
- For $\ell(n) = c \cdot n$, $c < 2$, padded RSA is conjectured secure, but no proof known
- For $\ell(n) = O(\log n)$, CPA security can be proven

- RSA Labs, Public-Key Crypto Standard PKCS #1, v1.5:
  
  $$c := \left( 0^8 || 0^610 || r || 0^8 || m \right)^e \mod N$$

  believed to be CPA secure, but CCA-attack is known
CCA security

\[
\text{challenger}
\]

\[
\text{PubK}_{A,\Pi}^{\text{cca}}(n)
\]

adversary \( A \)

\[
\begin{align*}
& m_0, m_1 \\
& \quad \leftarrow A^{\text{Enc}_{pk}(\cdot), \text{Dec}_{sk}(\cdot)}(pk) \\
& |m_0| = |m_1| \\
& b' \leftarrow A^{\text{Enc}_{pk}(\cdot), \text{Dec}_{sk}(\cdot)}(c)
\end{align*}
\]

adv \( A \) cannot ask to decrypt \( c \)!

\[
\begin{align*}
& \text{challenger} \\
& (pk, sk) \leftarrow \text{Gen}(1^n) \\
& b \leftarrow \{0, 1\} \\
& c \leftarrow \text{Enc}_{pk}(m_b) \\
& b = b' \\
& b \neq b' \\
& \downarrow 1 \\
& \downarrow 0
\end{align*}
\]
CCA Security Examples

1. Eve intercepts encrypted email to Bob, sends it to Bob herself. Bob answers to Eve and includes the decrypted email (i.e. acts as decryption oracle).

2. Alice & Eve participate in Bob’s auction. Alice bids $c = \text{Enc}(m)$. Due to CPA security, Eve does not learn $m$. However, Eve can bid $c' = \text{Enc}(2m)$ if $\text{Enc}$ is malleable.

- CCA-security $\Rightarrow$ Non-malleability
Optimal Asymmetric Encryption Padding

• Instead of PKCS #1 v1.5 padding, people use RSA-OAEP (Construction 13.9 in [KL])

- **Gen:** $(N, e, d) \leftarrow \text{GenRSA}(1^{n+1})$ 
  \[ || N || > 2n \]

- **Enc}_{pk}(m): \left[ m^e \mod N \right]$

- **Dec}_{sk}(c): \left[ c^d \mod N \right] = m = X||Y$
  check if final msg is of appropriate form

= $m$
Optimal Asymmetric Encryption Padding

Thm: If RSA-problem is hard wrt to GenRSA and G,H are independent random oracles. Then, RSA-OAEP is CCA-secure for $e=3$ (and other exponents)

$$\text{Gen: } (N,e,d) \leftarrow \text{GenRSA}(1^{n+1}) \quad || \quad N || > 2n$$

$$\text{Enc}_{pk}(m): \left[ m^e \mod N \right]$$

$$\text{Dec}_{sk}(c): \left[ c^d \mod N \right] = m = X||Y$$

check if final msg is of appropriate form
Recent Software Bugs

• Feb 2014: \texttt{#gotofail} in Apple software

• April 2014: \texttt{Heartbleed} in OpenSSL library, see \texttt{XKCD}

• 24 Sep 2014: \texttt{Shellshock} in Unix Bash shell

Bottom line: implementing security-related software is difficult