Introduction to Cryptology

Lecture 25
Announcements

• HW10 due next class (5/5)
• Extra credit due 5/5
• Stay tuned for survey about review session for final exam.
Agenda

• Last time:
  – Diffie-Hellman Key Exchange (10.3)
  – Public Key Encryption Definitions (11.2)
  – El Gamal Encryption (11.4)

• This time:
  – RSA Encryption and Weaknesses (11.5)
CONSTRUCTION 11.25

Let GenRSA be as in the text. Define a public-key encryption scheme as follows:

- **Gen**: on input $1^n$ run GenRSA($1^n$) to obtain $N, e$, and $d$. The public key is $\langle N, e \rangle$ and the private key is $\langle N, d \rangle$.

- **Enc**: on input a public key $pk = \langle N, e \rangle$ and a message $m \in \mathbb{Z}_N^*$, compute the ciphertext
  
  $$c := [m^e \mod N].$$

- **Dec**: on input a private key $sk = \langle N, d \rangle$ and a ciphertext $c \in \mathbb{Z}_N^*$, compute the message
  
  $$m := [c^d \mod N].$$

The plain RSA encryption scheme.
RSA Example

\[ p = 3, q = 7, N = 21 \]
\[ \phi(N) = 12 \]
\[ e = 5 \]
\[ d = 5 \]
\[ Enc_{(21,5)}(11) = 4^5 \mod 21 = 16 \mod 21 \]
\[ Dec_{21,5}(16) = 16^5 \mod 21 = 4^5 \cdot 4^5 \mod 21 \]
\[ = 16 \cdot 16 \mod 21 = 4 \]
Is Plain-RSA Secure?

• It is deterministic so cannot be secure!
Additional Attacks
Additional Attacks

Encrypting short messages using small $e$:

- When $m < N^{1/e}$, raising $m$ to the $e$-th power modulo $N$ involves no modular reduction.
- Can compute $m = c^{1/e}$ over the integers.
Additional Attacks

Encrypting a partially known message:

Coppersmith’s Theorem: Let $p(x)$ be a polynomial of degree $e$. Then in time $\text{poly}(\log(N), e)$ one can find all $m$ such that $p(m) = 0 \mod N$ and $m \leq N^{1/e}$.

In the following, we assume $e = 3$.
Assume message is $m = m_1 || m_2$, where $m_1$ is known, but not $m_2$.
So $m = 2^k \cdot m_1 + m_2$.
Define $p(x) := (2^k \cdot m_1 + x)^3 - c$.
This polynomial has $m_2$ as a root and $m \leq 2^k \leq N^{1/3}$. 
Additional Attacks

Encrypting related messages:
Assume the sender encrypts both $m$ and $m + \delta$, giving two ciphertexts $c_1$ and $c_2$.
Define $f_1(x) := x^e - c_1$ and $f_2(x) := (x + \delta)^e - c_2$.
$x = m$ is a root of both polynomials. $(x - m)$ is a factor of both.
Use algorithm for finding gcd of polynomials.
Additional Attacks

Sending the same message to multiple receivers:
\[ pk_1 = \langle N_1, 3 \rangle, \; pk_2 = \langle N_2, 3 \rangle, \; pk_3 = \langle N_3, 3 \rangle. \]
Eavesdropper sees:
\[ c_1 = m^3 \mod N_1, \; c_2 = m^3 \mod N_2, \; c_3 = m^3 \mod N_3 \]
Let \( N^* = N_1 \cdot N_2 \cdot N_3 \).
Using Chinese remainder theorem to find \( \hat{c} < N^* \) such that:
\[
\begin{align*}
\hat{c} &= c_1 \mod N_1 \\
\hat{c} &= c_2 \mod N_2 \\
\hat{c} &= c_3 \mod N_3.
\end{align*}
\]
Note that \( m^3 \) satisfies all three equations. Moreover, \( m^3 < N^* \). Thus, we can solve for \( m^3 = \hat{c} \) over the integers.
CONSTRUCTION 11.29

Let $\text{GenRSA}$ be as before, and let $\ell$ be a function with $\ell(n) \leq 2n - 4$ for all $n$. Define a public-key encryption scheme as follows:

- **Gen**: on input $1^n$, run $\text{GenRSA}(1^n)$ to obtain $(N, e, d)$. Output the public key $pk = \langle N, e \rangle$, and the private key $sk = \langle N, d \rangle$.

- **Enc**: on input a public key $pk = \langle N, e \rangle$ and a message $m \in \{0, 1\}_{\|N\| - \ell(n) - 2}$, choose a random string $r \leftarrow \{0, 1\}^{\ell(n)}$ and interpret $\hat{m} := 1||r||m$ as an element of $\mathbb{Z}_N^*$. Output the ciphertext
  \[ c := [\hat{m}^e \mod N]. \]

- **Dec**: on input a private key $sk = \langle N, d \rangle$ and a ciphertext $c \in \mathbb{Z}_N^*$, compute
  \[ \hat{m} := [c^d \mod N], \]
  and output the $\|N\| - \ell(n) - 2$ least-significant bits of $\hat{m}$.

The padded RSA encryption scheme.