RSA I

Security notions and schoolbook RSA

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Public-key cryptology

Public-key encryption requires 3 algorithms:

1. Key generation, generating a public-key private-key pair.
2. Encryption, taking a public key and a message, producing ciphertext.
3. Decryption, taking a private key and a ciphertext, producing plaintext.

Signatures also require 3 algorithms:

1. Key generation, generating a public-key private-key pair.
2. Signing, taking a private key and a message, producing a signature.
3. Verification, taking a public key and a signed message, producing valid or not.

Reminder: signatures and MACs both ensure authenticity and integrity.

But a signature can be verified by *anybody* using a public key
while MACs require *the same shared secret key.*

Signatures belong to public-key cryptography;
MACs belong to symmetric-key cryptography.

Encryption - formal security notions

Attacker goals

- Recover sk from pk.
- Recover m from $\text{Enc}_{\text{pk}}(m)$,
  i.e. break one-wayness (OW).
- Learn any information about plaintext (semantic security).

Encryption - formal security notions

Attacker goals

- Recover sk from pk.
- Recover m from $\text{Enc}_{\text{pk}}(m)$,
  i.e. break one-wayness (OW).
- Learn any information about plaintext (semantic security).
  Equivalent to breaking indistinguishability (IND),
  i.e., learning which of two attacker-chosen messages m_0, m_1 was encrypted in $c = \text{Enc}_{\text{pk}}(m_i)$ (beyond 50% chance of guessing.)

Attacker abilities

- Chosen plaintext attack (CPA)
  Attacker gets encryption of plaintexts of his choice.
- Chosen ciphertext attack (CCA I / II)
  Attacker can ask for decryptions of ciphertexts of his choice.
  For II the attacker can continue asking for decryptions after receiving a challenge ciphertext.

Schoolbook RSA encryption

1977 Rivest, Shamir, Adleman. Do not use Schoolbook RSA in practice!

Schoolbook RSA encryption

1977 Rivest, Shamir, Adleman. Do not use Schoolbook RSA in practice!

KeyGen:

1. Pick primes $p, q; p \neq q$.
2. Compute $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$.
3. Pick $1 < e < n$ with $\gcd(e, \varphi(n)) = 1$.
4. Compute $d \equiv e^{-1} \bmod \varphi(n)$.
5. Output public key (n, e), private key (n, d).

Schoolbook RSA encryption

1977 Rivest, Shamir, Adleman. Do not use Schoolbook RSA in practice!

KeyGen:

1. Pick primes $p, q; p \neq q$.
2. Compute $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$.
3. Pick $1 < e < n$ with $\gcd(e, \varphi(n)) = 1$.
4. Compute $d \equiv e^{-1} \bmod \varphi(n)$.
5. Output public key (n, e), private key (n, d).

Enc message $0 \leq m < n$:

1. Compute $c \equiv m^e \bmod n$. See video on Exponentiation, & slides
2. Output c.

Dec ciphertext $0 \leq c < n$:

1. Compute $m' \equiv c^d \bmod n$.
2. Output m'.

Schoolbook RSA encryption

1977 Rivest, Shamir, Adleman. Do not use Schoolbook RSA in practice!

KeyGen:

1. Pick primes $p, q; p \neq q$.
2. Compute $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$.
3. Pick $1 < e < n$ with $\gcd(e, \varphi(n)) = 1$.
4. Compute $d \equiv e^{-1} \bmod \varphi(n)$.
5. Output public key (n, e), private key (n, d).

Enc message $0 \leq m < n$:

1. Compute $c \equiv m^e \bmod n$.
2. Output c.

See video on Exponentiation, & slides

Dec ciphertext $0 \leq c < n$:

1. Compute $m' \equiv c^d \bmod n$.
2. Output m'.

Some k exists with $ed = 1 + k\varphi(n)$

Use Fermat's little theorem.

This works:

$$m' \equiv c^d \equiv (m^e)^d \equiv m^{ed} = m^{1+k\varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k \equiv m \cdot 1 \equiv m \bmod n.$$

Security analysis schoolbook RSA encryption

Attacker goals

- Learn any information about plaintext (semantic security).
  Equivalent to breaking Indistinguishability (IND),
  i.e., learning which of two attacker-chosen messages m_0, m_1 was encrypted in $c = \text{Enc}_{\text{pk}}(m_i)$ (beyond 50% chance of guessing.)

Attacker abilities

- Chosen plaintext attack (CPA)
  Attacker gets encryption of plaintexts of his choice.

Schoolbook RSA is not IND-CPA secure:
Attacker chooses two random messages m_0, m_1.
Challenger picks $b \in \{0, 1\}$ at random and sends back $c = \text{Enc}(m_b)$..

Security analysis schoolbook RSA encryption

Attacker goals

- Learn any information about plaintext (semantic security).
  Equivalent to breaking Indistinguishability (IND),
  i.e., learning which of two attacker-chosen messages m_0, m_1 was encrypted in $c = \mathrm{Enc}_{\mathrm{pk}}(m_i)$ (beyond 50% chance of guessing.)

Attacker abilities

- Chosen plaintext attack (CPA)
  Attacker gets encryption of plaintexts of his choice.

Schoolbook RSA is not IND-CPA secure:
Attacker chooses two random messages m_0, m_1.
Challenger picks $b \in \{0, 1\}$ at random and sends back $c = \mathrm{Enc}(m_b)$..

Schoolbook RSA is deterministic!
The attacker can just compute $m_0^e \bmod n$ and $m_1^e \bmod n$ and check which one matches c.

Not IND-CPA secure implies not IND-CCA secure.

RSA encryption is homomorphic

An encryption system is homomorphic if there exist operations $\circ$ on the ciphertext space and $\triangle$ on the message space so that

$$\mathrm{Enc}_k(m_1) \circ \mathrm{Enc}_k(m_2) = \mathrm{Enc}_k(m_1 \triangle m_2).$$

RSA encryption is homomorphic

An encryption system is homomorphic if there exist operations $\circ$ on the ciphertext space and $\triangle$ on the message space so that

$$\mathrm{Enc}_k(m_1) \circ \mathrm{Enc}_k(m_2) = \mathrm{Enc}_k(m_1 \triangle m_2).$$

For RSA we have

$$c_1 \cdot c_2 \equiv m_1^e \cdot m_2^e \equiv (m_1 \cdot m_2)^e \bmod n,$$

so RSA is homomorphic with $\circ = \triangle$ being multiplication modulo n.

RSA encryption is homomorphic

An encryption system is homomorphic if there exist operations $\circ$ on the ciphertext space and $\triangle$ on the message space so that

$$\mathrm{Enc}_k(m_1) \circ \mathrm{Enc}_k(m_2) = \mathrm{Enc}_k(m_1 \triangle m_2).$$

For RSA we have

$$c_1 \cdot c_2 \equiv m_1^e \cdot m_2^e \equiv (m_1 \cdot m_2)^e \bmod n,$$

so RSA is homomorphic with $\circ = \triangle$ being multiplication modulo n.

Homomorphic properties can be desired, so this is not strictly a problem, but it's important to be aware of them.

Security requirements

Attacker goals

- Recover m from $\mathrm{Enc}_{\mathrm{pk}}(m)$,
  i.e. break one-wayness (OW).

Attacker abilities

- Chosen ciphertext attack (CCA I / II)
  Attacker can ask for decryptions of ciphertexts of his choice.
  For II the attacker can continue asking for decryptions after receiving a challenge ciphertext.

Security requirements

Attacker goals

- Recover m from $\text{Enc}_{\text{pk}}(m)$,
  i.e. break one-wayness (OW).

Attacker abilities

- Chosen ciphertext attack (CCA I / II)
  Attacker can ask for decryptions of ciphertexts of his choice.
  For II the attacker can continue asking for decryptions after receiving a challenge ciphertext.

Homomorphic systems cannot be OW-CCA II secure:

Security requirements

Attacker goals

- Recover m from $\mathrm{Enc}_{\mathrm{pk}}(m)$,
  i.e. break one-wayness (OW).

Attacker abilities

- Chosen ciphertext attack (CCA I / II)
  Attacker can ask for decryptions of ciphertexts of his choice.
  For II the attacker can continue asking for decryptions after receiving a challenge ciphertext.

Homomorphic systems cannot be OW-CCA II secure:
Pick random message r compute $c_r = \mathrm{Enc}_{\mathrm{pk}}(r)$ and submit

$$c \neq c' = c_r \circ c = \mathrm{Enc}_{\mathrm{pk}}(r) \circ \mathrm{Enc}_{\mathrm{pk}}(m) = \mathrm{Enc}_{\mathrm{pk}}(r \triangle m)$$

for decryption.

Security requirements

Attacker goals

- Recover m from $\mathrm{Enc}_{\mathrm{pk}}(m)$,
  i.e. break one-wayness (OW).

Attacker abilities

- Chosen ciphertext attack (CCA I / II)
  Attacker can ask for decryptions of ciphertexts of his choice.
  For II the attacker can continue asking for decryptions after receiving a challenge ciphertext.

Homomorphic systems cannot be OW-CCA II secure:
Pick random message r compute $c_r = \mathrm{Enc}_{\mathrm{pk}}(r)$ and submit

$$c \neq c' = c_r \circ c = \mathrm{Enc}_{\mathrm{pk}}(r) \circ \mathrm{Enc}_{\mathrm{pk}}(m) = \mathrm{Enc}_{\mathrm{pk}}(r \triangle m)$$

for decryption. From $r \triangle m$ recover m.

The fine print: This requires $\triangle$ to be an operation so that m can be recovered from $r \triangle m$ and r. Note that the attacker has no restrictions in choosing r other than $c' \neq c$.

RSA OAEP – Optimal asymmetric encryption padding

Let modulus n have ℓ bits. Messages have $\ell - k_0 - k_1$ bits.

OAEP appends $k_0 + k_1$ bits to message m.

There are k_1 bits all equal to zero and k_0 random bits in r.

G is cryptographic hash function $\{0,1\}^{k_0} \to \{0,1\}^{\ell - k_0}$.
H is cryptographic hash function $\{0,1\}^{\ell - k_0} \to \{0,1\}^{k_0}$.

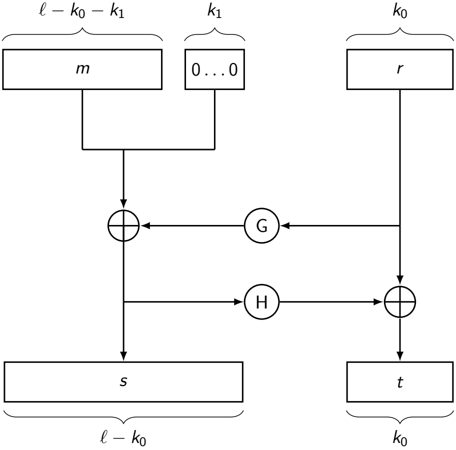

Image credit: adapted from Matthieu Giraud

RSA OAEP first computes $M = (s, t)$, the OAEP encoding of m.
Then encrypts M as M^e mod n. RSA OAEP is CCA-II secure.