TUTORIAL

CSCI361 – Computer Security

Sionggo Japit
sjapit@uow.edu.au

12 February 2024

RSA

Chosen ciphertext attack

Chosen ciphertext attack

RSA is insecure against chosen ciphertext attack. Explain or show by example that RSA is insecure against chosen ciphertext attack.

Chosen ciphertext attack

An adversary wants to decrypt C, a ciphertext, in the form of $C = m^e \bmod n$, to obtain the plaintext m. For example, Alice sends y to Bob and Charlie (the adversary) want to know what message Alice sends.

Chosen ciphertext attack

- The adversary, Charlie, creates a random message m_1 such that $\gcd(m_1, n) = 1$.
- Charlie then encrypts the message m_1 to produce a ciphertext $C_1 = m_1^e \bmod n$. (C_1 is a chosen ciphertext.)
- Charlie then creates a new ciphetext $C_2 = C_1$ ´ C.

Chosen ciphertext attack

- Charlie sends C_2 to Bob, and asks Bob to decrypt, saying he wants to test if his encryption is correct. Tricked to believe Charlie, Bob decrypts C_2 and sends m_2 to Charlie. ($m_2 = C_2^d \bmod n$)
- Since $C_2 = C_1 \text{´} C$, and $C_2 = m_2^e \bmod n$, Charlie can compute $m_2^e = m_1^e \text{´} m^e \bmod n$.

$$(Note: C_2 = m_2^e \bmod n, C_1 = m_1^e \bmod n, and\ C = m^e \bmod n)$$

Chosen ciphertext attack

$$m_2^e = m_1^e \times m^e \bmod n$$

$$m_2 = m_1 \times m \bmod n$$

$$m = \frac{m_2}{m_1} \bmod n$$

$$m = m_2 \times m_1^{-1} \bmod n$$

Since $\gcd(m_1, n) = 1$, m^{-1} can be computed using extended Euclidean algorithm. Charlie also receives m_2 from Bob, and hence m can be computed easily.

ElGamal

Chosen ciphertext attack

Chosen ciphertext attack

ElGamal is insecure against chosen ciphertext attack. Explain or show by example that ElGamal is insecure against chosen ciphertext attack.

Chosen ciphertext attack

An attacker wants to decrypt a target ciphertext message C, which consists of $C = (c_1, c_2)$, where $c_1 = g^{k_1} \bmod p$, and $c_2 = m \times (y_2)^{k_1} = m \times K \bmod p$, to obtain a plaintext m.

For example, Alice sends C to Bob and Charlie (the adversary) wants to know what message Alice sends.

(Note:

k_1 = Alice's private key,

y_2 = Bob's public key, which equals g^{k_2}, and

$K = (y_2)^{k_1} = (g^{k_2})^{k_1}$ is a common key)

Chosen ciphertext attack

- The attacker randomly chooses r such that $\gcd(r, p) = 1$, and computes $c_3 = r \times c_2$; c_3 is the chosen ciphertext.
- The attacker then sends $(c_1,\ c_3)$ to Bob asking Bob to decrypt, saying he wants to test if his encryption is correct.
- Tricked to believe the attacker, Bob decrypts the ciphertext c_3 and sends m_3 to the attacker.

Chosen ciphertext attack

- The attacker then computes:
  - $K = c_1^{k_2} = \left(g^{k_1}\right)^{k_2} = g^{k_1 k_2}$
  - K^{-1} using extended Euclidean algorithm
  - $m_3 = \dfrac{c_3}{K} = c_3 \times K^{-1} \bmod p$
  - $m_3 = \dfrac{r \times c_2}{K} = r \times c_2 \times K^{-1} \bmod p$ Since $c_3 = r \times c_2$
  - $m_3 = r \times m \times K \times K^{-1} \bmod p$ and since $c_2 = m \times K$
  - $m_3 = r \times m$

Chosen ciphertext attack

\ m can be computed as $m = r^{-1}$ ´ m_3.

(Note: The attacker has m_3 from Bob, r and r^{-1} are decided by the attacker. Hence m can be computed.)