Number theory and Cryptography May 24th, 2024

Lecture 6 :The RSA Cryptosystem

Instructor: Chao Qin *Notes written by: Wenhao Tong and Yingshu Wang*

All classical ciphers, including shift and affine ciphers, are private key cryptosystems. Knowing the encryption key allows one to quickly determine the decryption key. All parties who wish to communicate using a private key cryptosystem must share the key and keep it a secret. In public key cryptosystems, first invented in the 1970s, knowing how to encrypt a message does not help one to decrypt the message. Therefore, everyone can have a publicly known encryption key. The only key that needs to be kept secret is the decryption key.

A public key cryptosystem, now known as the RSA system was introduced in 1976 by three researchers at MIT. It is now known that the method was discovered earlier by Clifford Cocks, working secretly for the UK government.

The public encryption key is (n, e), where $n = pq$ (the modulus) is the product of two large (200 digits) primes p and q, and an exponent e that is relatively prime to $(p-1)(q-1)$. The two large primes can be quickly found using probabilistic primality tests, discussed earlier. But $n = pq$, with approximately 400 digits, cannot be factored in a reasonable length of time.

1 The RSA Cryptosystem

1.1 RSA Encryption

To encrypt a message using RSA using a key (n, e) :

1. Translate the plaintext message M into sequences of two-digit integers representing the letters. Use 00 for A, 01 for B, etc.

2. Concatenate the two-digit integers into strings of digits.

3. Divide this string into equally sized blocks of 2N digits where 2N is the largest even number 2525. . . 25 with 2N digits that does not exceed n.

4. The plaintext message M is now a sequence of integers $m_1, m_2, \ldots, m_k$.

5. Each block (an integer) is encrypted using the function $C = M^e \; mod \; n$.

Example 1. *Encrypt the message STOP using the RSA cryptosystem with key* $(2537, 13)$.

- $2537 = 43 \cdot 59$,

- $p = 43$ *and* $q = 59$ *are primes and* $gcd(e, (p-1)(q-1)) = gcd(13, 42 \cdot 58) = 1$.

Solution 1. *Translate the letters in STOP to their numerical equivalents 18 19 14 15.*

- *Divide into blocks of four digits (because 2525 < 2537 < 252525) to obtain 1819 1415.*

- *Encrypt each block using the mapping* $C = M^{13} \pmod{2537}$.

- *Since* $1819^{13} \pmod{2537} = 2081$ *and* $1415^{13} \pmod{2537} = 2182$*, the encrypted message is* 20812182.

1.2 RSA Decryption

- To decrypt a RSA ciphertext message, the decryption key d, an inverse of e modulo $(p-1)(q-1)$ is needed. The inverse exists since $gcd(e, (p-1)(q-1)) = gcd(13, 42 \cdot 58) = 1$.

- With the decryption key d, we can decrypt each block with the computation M = C^d mod $p \cdot q$.

- RSA works as a public key system since the only known method of finding d is based on a factorization of n into primes. There is currently no known feasible method for factoring large numbers into primes.

Example 2. *The message 0981 0461 is received. What is the decrypted message if it was encrypted using the RSA cipher from the previous example?*

Solution 2. *The message was encrypted with* $n = 43 \cdot 59$ *and exponent 13. An inverse of 13 modulo* $42 \cdot 58 = 2436$ *is* d *= 937.*

- *To decrypt a block C, M =* C^{937} *mod 2537.*
- *Since* 0981^{937} *mod 2537 = 0704 and* 0461^{937} *mod 2537 = 1115, the decrypted message is 0704 1115. Translating back to English letters, the message is HELP.*

1.3 Cryptographic Protocols: Key Exchange

- Cryptographic protocols are exchanges of messages carried out by two or more parties to achieve a particular security goal.
- Key exchange is a protocol by which two parties can exchange a secret key over an insecure channel without having any past shared secret information. Here the Diffe-Hellman key agreement protocol is described by example.

  1. Suppose that Alice and Bob want to share a common key.
  2. Alice and Bob agree to use a prime p and a primitive root a of p.
  3. Alice chooses a secret integer k_1 and sends a^{k1} mod p to Bob.
  4. Bob chooses a secret integer k_2 and sends a^{k2} mod p to Alice.
  5. Alice computes $(a^{k2})^{k1}$ mod p.
  6. Bob computes $(a^{k1})^{k2}$ mod p.

- At the end of the protocol, Alice and Bob have their shared key
- $(a^{k2})^{k1}$ mod p = $(a^{k1})^{k2}$ mod p.
- To find the secret information from the public information would require the adversary to find k_1 and k_2 from a^{k_1} mod p and a^{k_2} mod p respectively. This is an instance of the discrete logarithm problem, considered to be computationally infeasible when p and a are sufficiently large.

1.4 Cryptographic Protocols: Digital Signatures

- Adding a digital signature to a message is a way of ensuring the recipient that the message came from the purported sender.
- Suppose that Alice's RSA public key is (n, e) and her private key is d. Alice encrypts a plain text message x using $E_{(n,e)}(x) = x^d \bmod n$. She decrypts a ciphertext message y using $D_{(n,e)}(y) = y^d \bmod n$.
- Alice wants to send a message M so that everyone who receives the message knows that it came from her.
  1. She translates the message to numerical equivalents and splits it into blocks, just as in RSA encryption.
  2. She then applies her decryption function $D_{(n,e)}$ to the blocks and sends the results to all intended recipients.
  3. The recipients apply Alice's encryption function and the result is the original plain text since $E_{(n,e)}(D_{(n,e)}(x)) = x$.
- Everyone who receives the message can then be certain that it came from Alice.

Example 3. *Suppose Alice's RSA cryptosystem is the same as in the earlier example with key(2537,13), 2537= 43· 59, p = 43 and q = 59 are primes and gcd(e,(p-1)(q-1)) = gcd(13, 42· 58) = 1.*
Her decryption key is d = 937.
She wants to send the message "MEET AT NOON" to her friends so that they can be certain that the message is from her.

Solution 3. *Alice translates the message into blocks of digits 1204 0419 0019 1314 1413*

1. *She then applies her decryption transformation $D_{(2537,13)}$ (x)= x^{937} mod 2537 to each block*
2. *She finds (using her laptop, programming, and knowledge of discrete mathematics) that 1204^{937} mod 2537 = 817, 419^{937} mod 2537 = 555 , 19^{937} mod 2537= 1310, 1314^{937} mod 2537= 2173, and 1413^{937} mod 2537 = 1026*
3. *She sends 0817 0555 1310 2173 1026*

- When one of her friends receive the message, they apply Alice's encryption transformation $E_{(2537,13)}$ to each block. They then obtain the original message which they translate back to English letters.