INFORMATION & COMPUTER SCIENCES
UNIVERSITY of HAWAI'I at MĀNOA

Ch 4.6: Cryptography

ICS 141: Discrete Mathematics for Computer Science I

KYLE BERNEY
DEPARTMENT OF ICS, UNIVERSITY OF HAWAII AT MANOA

Terminology

- Cryptography is the study of transforming information so that it cannot be easily recovered without special knowledge

- Encryption is the process of making a message secret
- Decryption is the process of determining the original messsage from the encrypted message

- Cryptosystem is a set of algorithms and protocols used to implement a particular security service
  - Encryption algorithm
  - Decryption algorithm
  - Key generation algorithm

Caesar Cipher

- One of the earliest known uses of cryptography used by Julius Caesar
- Encrypt messages by shifting each letter by a fixed amount

- Represent each letter by an integer in $\{0, 1, \ldots, 25\}$
- Define a function to encode each letter

$$f(x) = (x + 3) \pmod{26}$$

- Use the inverse function to decrypt each letter

$$f^{-1}(x) = (x - 3) \pmod{26}$$

Caesar Cipher

- One of the earliest known uses of cryptography used by Julius Caesar
- Encrypt messages by shifting each letter by a fixed amount

- Represent each letter by an integer in $\{0, 1, \ldots, 25\}$
- Define a function to encode each letter

$$f(x) = (x + 3) \pmod{26}$$

- Use the inverse function to decrypt each letter

$$f^{-1}(x) = (x - 3) \pmod{26}$$

- Ex: "HELLO WORLD" $\Leftrightarrow$ "KHOOR ZRUOG"

Affine Cipher

- Generalization of a Caesar cipher
- Let a and b be integers
- Use a bijection function f such that

$$f(x) = ax + b \pmod{26}$$

where a has an inverse modulo 26

$$\Rightarrow \mathrm{GCD}(a, 26) = 1$$

- Suppose that $y = ax + b \pmod{26}$, then to decrypt

$$x \equiv (y - b)a^{-1} \pmod{26}$$

Transposition Cipher

- Define a permutation $\sigma : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\}$
- To encrypt a message:
  1. Split the letters of the message into blocks of m letters
  2. Use σ to permute each of the blocks of m letters
- To decrypt a message:
  1. Split the letters of the message into blocks of m letters
  2. Use the inverse permutation, σ^{-1} to permute each of the blocks of m letters

Transposition Cipher

- Ex: Given $\sigma : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ such that $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, and $\sigma(4) = 2$. Encrypt the message "PIRATE ATTACK"

Transposition Cipher

- Ex: Given $\sigma : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ such that $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, and $\sigma(4) = 2$. Encrypt the message "PIRATE ATTACK"

- Solution:

  1. Split the message into blocks of 4 letters:
     "PIRA TEAT TACK"
  2. Permute each block using σ to obtain:
     "IAPR ETTA AKTC"

Private Key Cryptography

- The previous ciphers are all examples of private key cryptosystems
  - Once the encryption key is known, you can quickly decrypt the message
- Caesar Cipher: f defines the encryption key
- Affine Cipher: f defines the encryption key
- Transposition Cipher: σ defines the encryption key
- When a private key crypotosystem is used, two parties who communicate must share a secret key
- A modern example is the Advanced Encryption Standard (AES)

Public Key Cryptosystems

- In a public key cryptosystem, knowing how to send an encrypted message does not help decrypt messages
  - Everyone can have a publicaly known encryption key
  - Only the decryption key is kept secret
- Advantage:
  - Two parties do not need to exchange keys
- Disadvantage:
  - Encryption and decryption can be time-consuming
- For applications that require encryption and decryption to be time-sensitive, private key cryptosystems are used
  - Public key cryptosystems may be used to exchange private keys

RSA Cryptosystem

- Introduced by three MIT researchers in 1977
  - Ronald Rivest
  - Adi Shamir
  - Leonard Adleman
- Developed by Clifford Cocks, working in secret at the UK's Goverment Communications Headquarters in 1973
  - Declassified in 1997

RSA Cryptosystem

- Basic idea is the observation that it is practical to find three very large positive integers, e, d, and n such that
  - For all integers m, where $0 \leq m < n$
  - $(m^e)^d \equiv m \pmod{n}$
- However, when given only e and n, it is very difficult to find d
- To encrypt a message m:

$$m^e \pmod{n}$$

- To decrypt a message m^e:

$$(m^e)^d \equiv m \pmod{n}$$

- n and e comprise the public key
- d represents the private key

RSA Cryptosystem

- Keys are generated as follows:
  1. Choose two large prime numbers p and q
  2. Compute $n = pq$
  3. Compute $\lambda(n)$, called the Carmichael's totient function
     - $\lambda(n) = \text{LCM}(p-1, q-1)$
  4. Choose an integer e such that
     - $1 < e < \lambda(n)$
     - $\text{GCD}(e, \lambda(n)) = 1$, i.e., they are coprime
  5. Compute $d \equiv e^{-1} \pmod{\lambda(n)}$
     - Equivalent to solving the equation

$$de \equiv 1 \pmod{\lambda(n)}$$

RSA Cryptosystem

- Keys are generated as follows:
  1. Choose two large prime numbers p and q
  2. Compute $n = pq$
  3. Compute $\lambda(n)$, called the Carmichael's totient function
     - $\lambda(n) = \text{LCM}(p-1, q-1)$
  4. Choose an integer e such that
     - $1 < e < \lambda(n)$
     - $\text{GCD}(e, \lambda(n)) = 1$, i.e., they are coprime
  5. Compute $d \equiv e^{-1} \pmod{\lambda(n)}$
     - Equivalent to solving the equation

$$de \equiv 1 \pmod{\lambda(n)}$$

- *Remark:* In the original RSA paper, the Euler totient function $\phi(n) = (p-1)(q-1)$ is used instead of $\lambda(n)$,

RSA Cryptosystem

- Computing/finding the private key d requires knowledge of the large primes p and q
- Factoring $n = pq$ cannot be done (currently) in a reasonable length of time
  - Theoretical factorization algorithms have been developed for quantum computers that may be used in the future
- In comparision, finding large primes p and q to generate the keys can be done relatively fast using primality testing algorithms