Number theory and Cryptography May 21st, 2024

Lecture 5 : Public-key Cryptography

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

1 Classical Cryptography

1.1 Caesar Cipher

Julius Caesar created secret messages by shifting each letter three letters forward in the alphabet (sending the last three letters to the first three letters). For example, B is replaced by E and X is replaced by A. This process of making a message secret is an example of encryption.
Here is how the encryption process works:

- Replace each letter by an integer from $\mathbb{Z}_{26}$, that is an integer from 0 to 25 representing one less than its position in the alphabet.
- The encryption function is $f(p) = (p + 3) \pmod{26}$. It replaces each integer p in the set $\{0, 1, 2, \ldots, 25\}$ by $f(p)$ in the set $\{0, 1, 2, \ldots, 25\}$.
- Replace each integer p by the letter with the position $p + 1$ in the alphabet.

Example 1. *Encrypt the message "MEET YOU IN THE PARK" using the Caesar cipher.*

Solution 1. *12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10*
Now replace each of these numbers p by $f(p) = (p + 3) \pmod{26}$.
15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13
Translating the numbers back to letters produces the encrypted message "PHHW BRX LQ WKH SDUN.

- To recover the original message, use $f^{-1}(p) = (p - 3) \pmod{26}$. So, each letter in the coded message is shifted back three letters in the alphabet, with the first three letters sent to the last three letters. This process of recovering the original message from the encrypted message is called decryption.

- The Caesar cipher is one of a family of ciphers called shift ciphers. Letters can be shifted by an integer k, with 3 being just one possibility. The encryption function is

$$f(p) = (p + k) \pmod{26}$$

and the decryption function is

$$f^{-1}(p) = (p - k) \pmod{26}$$

- The integer k is called a key.

1.2 Shift Cipher

Example 2. *Encrypt the message "STOP GLOBAL WARMING" using the shift cipher with $k = 11$.*

Solution 2. *Replace each letter with the corresponding element of $\mathbb{Z}_{26}$.*
18 19 14 15 6 11 14 1 0 11
Apply the shift $f(p) = (p + 11) \pmod{26}$, yielding
3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17
Translating the numbers back to letters produces the ciphertext "DEZA RWZMLW HLCXTYR."

Example 3. *Decrypt the message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted using the shift cipher with $k = 7$.*

Solution 3. *Replace each letter with the corresponding element of $\mathbb{Z}_{26}$.*
11 4 22 11 24 15 11 20 9 1 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24
Shift each of the numbers by $-k$ = -7 modulo 26, yielding
4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17
Translating the numbers back to letters produces the decrypted message "EXPERIENCE IS A GREAT TEACHER."

1.3 Affine Ciphers

Shift ciphers are a special case of affine ciphers which use functions of the form $f(p) = (ap + b) \pmod{26}$, where a and b are integers, chosen so that f is a bijection.The function is a bijection if and only if $gcd(a, 26) = 1$.

Example 4. *What letter replaces the letter K when the function* $f(p) = (7p + 3) mod 26$ *is used for encryption.*

Solution 4. *Since 10 represents K,* $f(10) = (7 \cdot 10 + 3) \bmod 26 = 21$*, which is then replaced by V. To decrypt a message encrypted by a shift cipher, the congruence* $c \equiv ap + b \pmod{26}$ *needs to be solved for* p*.*

- *Subtract* b *from both sides to obtain* $c - b \equiv ap \pmod{26}$*.*
- *Multiply both sides by the inverse of* a *modulo 26, which exists since* $gcd(a, 26) = 1$*.*
- $\overline{a}(c - b) \equiv \overline{a}ap \pmod{26}$*, which simplifies to* $\overline{a}(c - b) \equiv p \pmod{26}$*.*
- $p \equiv \overline{a}(c - b) \pmod{26}$ *is used to determine* p *in* $\mathbb{Z}_{26}$*.*

1.4 Block Ciphers

- A simple type of block cipher is called the transposition cipher.The key is a permutation σ of the set $\{1, 2, \ldots, m\}$, where m is an integer, that is a one-to-one function from $\{1, 2, \ldots, m\}$ to itself.
- To encrypt a message, split the letters into blocks of size m, adding additional letters to fill out the final block. We encrypt $p_1, p_2, \ldots, p_m$ as $c_1, c_2, \ldots, c_m = p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(m)}$.
- To decrypt the $c_1, c_2, \ldots, c_m$ transpose the letters using the inverse permutation σ^{-1}

Example 5. *Using the transposition cipher based on the permutation* σ *of the set* $\{1, 2, 3, 4\}$ *with* $\sigma(1) = 3$ *,* $\sigma(2) = 1$*,* $\sigma(3) = 4$ *,* $\sigma(4) = 2$*,*
a*. Encrypt the plaintext PIRATE ATTACK*
b*. Decrypt the ciphertext message SWUE TRAEOEHS, which was encrypted using the same cipher.*

Solution 5. a*. Split into four blocks PIRA TEAT TACK.Apply the permutation* σ *giving IAPR ETTA AKTC*
b*.* $\sigma^{-1}(1) = 2$*,* $\sigma^{-1}(2) = 4$*,* $\sigma^{-1}(3) = 1$*,* $\sigma^{-1}(4) = 3$*.*
Apply the permutation σ^{-1} *giving USEW ATER HOSE.Split into words to obtain USE WATER HOSE.*

1.5 Cryptosystems

Definition. *A cryptosystem is a five-tuple (P,C,K,E,D), where*

- *P is the set of plaintext strings,*
- *C is the set of ciphertext strings,*
- *K is the keyspace (set of all possible keys),*
- *E is the set of encryption functions, and*
- *D is the set of decryption functions.*
- The encryption function in E corresponding to the key k is denoted by E_k and the description function in D that decrypts cipher text encrypted using E_k is denoted by D_k.Therefore:
- $D_k(E_k(p)) = p$, for all plaintext strings p.

Example 6. *Describe the family of shift ciphers as a cryptosystem.*

Solution 6. *Assume the messages are strings consisting of elements in* $\mathbb{Z}_{26}$.

- *P is the set of strings of elements in*$\mathbb{Z}_{26}$.
- *C is the set of strings of elements in* $\mathbb{Z}_{26}$,
- $K = \mathbb{Z}_{26}$,
- *E consists of functions of the form* $E_k(p) = (p - k)$ *mod 26 , and*
- *D is the same as E where* $D_k(p) = (p - k)$ *mod 26 .*