§ 4.6 Encryption

Jessica Wei

Encryption

DEF | Encryption The process by which a message is made secret.

Classic Cryptography

I. Shift and Affine Ciphers

Process

1. Assign a numeric value to each letter
   $A, B, ..., Z \Rightarrow 00, 01, ...25$

2. Apply a shift k to the value that only the intended recipient knows about

Example 1. Julius Cesar

Encrypted messages by shifting each letter three letters over. Use this shift to encrypt

"MEET YOU IN THE PARK"

1. M E E T Y O U I N T H E P A R K
   12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

2. 15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13
   Answer: PHHW BRX LQ RXL QWKHSDUN

For this particular example, we can express an encryption function that describes the rule applied to each letter:

$$f(x) = p + 3 \mod 26$$

where $p \in 00, 01, ..., 25$

NOTE: This cipher is not very secure because you can break it by:

i) Brute Force: test every one of the 26 possible shifts

ii) checking letter frequencies w/ popular letters

***Encryption Function:**

We can further generalize the encryption function to be of the form:

$$f(p) = ap + b \mod 26$$

where $a, b \in \mathbb{Z}$ and $\gcd(a, 26) = 1$.

This last condition ensures that the function is bijective. (i.e. that there will be an inverse function to decrypt)

* If $a = 1$, $f(p) = p + b \mod 26$, then we have a shift cipher with key b

* If $a > 1$, then we call the function an affine transformation.

The key is necessary for easy decryption.

***Decryption Function:**
Case: Shift Cipher

$$f^{-1}(q) = q - b \mod 26$$

Case: Affine Transformation

$$q = ap + b \mod 26 \Rightarrow ap + b = q \mod 26$$
$$ap \equiv q - b \mod 26$$

Since $\gcd(a, 26) = 1$, $\exists \bar{a} \in \mathbb{Z}$

$$\bar{a}ap \equiv \bar{a}(q - b) \mod 26$$
$$\Rightarrow p \equiv \bar{a}(q - b) \mod 26$$

$\therefore$ Decryption Function $= f^{-1}(q) = \bar{a}(q - b) \mod 26$

Example 2. An Affine transformation was applied with $a = 7$ and $b = 3$ to encode a letter. The encrypted letter is V. What was the original letter? *Note V = 21

$$f^{-1}(q) = \bar{a}(q - 3) \mod 26$$

Need: Inverse of $7 \mod 26$

$26 = 3 \cdot 7 + 5 \Rightarrow 5 = 26 - 3 \cdot 7$

$7 = 1 \cdot 5 + 2 \Rightarrow 2 = 7 - 5$

$5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2$

$2 = 2 \cdot 1 + 0$

———

$1 = 5 - 2(7 - 5) = 3 \cdot 5 - 2 \cdot 7$

$1 = 3(26 - 3 \cdot 7) - 2 \cdot 7 = 3 \cdot 26 - 11 \cdot 7$

inverse = -11 = $15 \mod 26 \Rightarrow \bar{a} = 15$

———

$f^{-1}(q) = 15(q - 3) \mod 26$

$f^{-1}(21) = 15(21 - 3) \mod 26$

$= 15 \cdot 18 \mod 26 = 45 \cdot 6 \mod 26$

$= (45 \mod 26)(6 \mod 26) = 114 \mod 26 = 10$

Answer: k

II. Transportation Ciphers Process

1. Divide the string of letters into blocks of a given size and add a padding in the last block if necessary (xx)

2. Permute the letters of each block

Example 3. Use the permutation $\sigma : 1, 2, 3, 4$ defined by $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 2$ to encrypt the message "PIRATE ATTACK".

1. PIRA TEAT TACK

2. IAPR ETTA AKTC

Answer: IAPRETTAAKTC

Example 4. Decrypt the message SWUE TRAE OEHS if the encryption that was used $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 2$

$\sigma^{-1}(1) = 2$, $\sigma^{-1}(2) = 4$, $\sigma^{-1}(3) = 4$, $\sigma^{-1}(4) = 3$

USEW ATER HOSE

Answer: Use Water Hose

DEF | Cryptosystem
A cryptosystem is a 5-tuple (P, C, K, E, D) where

P: set of plaintext strings

C: set of ciphertext strings

K: set of possible keys

E: set of encryption functions

D: set of decryption functions

Given some key $k \in K$

· $E_k \in E$ is an encryption function with key K

· $D_k \in D$ is a decryption function with key K

Example 5. Describe the family of shift ciphers as a cryptosystem.

$C = K = P = 00, 01, ..., 25 = \mathbb{Z}_{26}$

$E = p + b \mod 26 | q, b \in \mathbb{Z}_{26}$

$D = q - b \mod 26 | q, b \in \mathbb{Z}_{26}$

RSA

DEF | Private Cryptosystem
A cryptosystem where knowing a key allows you to find the decryption function.

DEF | Public Cryptosystem
A cryptosystem where knowing a key does not reveal the decryption function.

Key: (n, e) where $n, e \in \mathbb{Z}$
(i) $n = p \cdot q$ where $p, q \in \mathbb{Z}$ primes(200+ digits)

(ii) e satisfies $\gcd(e,\ (p-1)(q-1)) = 1$

Encryption Function:

$$c = m^e \mod n$$

Process:

1. $A, B, ...Z \Rightarrow 00, 01, ...25$
2. Concatenate the digits into blocks of even size (all blocks must be the same size)
   *In practical applications, the block size depends on key size
   *In our case, adopt the convention that size = # of digits in 2525..25 where 2525..25< n
   e.g. $n = 3821 \Rightarrow 2525 < 3821 \Rightarrow 5 = 4$
3. Apply the encryption function to each block m_i

$$c_i = m_i^e \mod n$$

4. Concatenate the cipher block c

Example 6. Encrypt "STOP", key: (2537,13)

1. STOP $\rightarrow$ 18191415
2. $n = 2547$, $2525 < 2537 \Rightarrow$ size $= 4$
   $m_1 = 1819$, $m_2 = 1415$
3. $c_1 = 1819^{13} \mod 2537 = 2081$
   $c_2 = 1415^1 3 \mod 2537 = 2182$
4. **Cipher:** 20812182

Decryption
***Goal:** $c = m^e \mod n$ obtain $m \in$ plaintext digits
Information about key:

(1) $n = p \cdot q$ where p, q are primes

(2) $\gcd(e, (p-1)(q-1)) = 1$

Consider (2), we are able to find an inverse of $e, \bar{e}_i \mod (p-1)(q-1)$ i.e.

$$e\bar{e} - 1 = (p-1)(q-1)k \qquad k \in \mathbb{Z}$$
$$e\bar{e} = (p-1)(q-1)k + 1$$
$$c \equiv m^e \mod n$$
$$c^{\bar{e}} \equiv (m^e)^{\bar{e}} \mod n$$
$$c^{\bar{e}} \equiv m^{e\bar{e}} \mod n$$
$$c^{\bar{e}} \equiv m^{(p-1)(q-1)k+1} \mod n \qquad m^{a+b} \equiv m^a \cdot m^b$$
$$c^{\bar{e}} \equiv m^{(p-1)(q-1)k} \mod n$$
$$\Rightarrow c^{\bar{e}} - m^{(p-1)(q-1)k} \cdot m = ny \qquad y \in \mathbb{Z}$$
$$\Rightarrow c^{\bar{e}} = ny + m^{(p-1)(q-1)k} \cdot m$$
$$\Rightarrow c^{\bar{e}} = pqy + m^{(p-1)(q-1)k} \cdot m$$
$$\Rightarrow c^{\bar{e}} = m^{(p-1)(q-1)k} \cdot m \mod p$$
$$\Rightarrow c^{\bar{e}} = m^{(p-1)(q-1)k} \cdot m \mod q$$

Recall FLT: If p is prime & $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$
Case 1. $p \nmid m$ and $q \nmid m$
$m^{p-1} \equiv 1 \mod p$ and $m^{q-1} \equiv 1 \mod q$ (5)
Hence by (5), we obtain the system

$$c^{\bar{e}} = (m^{(p-1)})^{(q-1)k} \cdot m \mod p = 1^{(q-1)k} \cdot, \quad \mod p \equiv m \mod p$$

$$\Rightarrow c^{\bar{e}} \equiv m \mod p$$
$$*c^{\bar{e}} \equiv (m^{(q-1)})^{(p-1)k} \cdot m \mod q \equiv 1^{(q-1)k} \cdot m \mod q$$
$$c^{\bar{e}} \equiv m \mod q$$
$$c^{\bar{e}} \equiv m \mod p$$
$$c^{\bar{e}} \equiv m \mod q$$

Solve this System of Congruence to obtain plaintext block m Solving by substitution results in the substitution

$$m = c^{\bar{e}} \mod n$$

Case 2. $p|m$ or $q|m$ (rarely ever happens)
Use CRT to show that

$$c^{\bar{e} \equiv m^{(p-1)(q-1)k}} \cdot m \mod p$$

$$c^{\bar{e} \equiv m^{(p-1)(q-1)k}} \cdot m \mod q$$

still results in the same decryption function.

Summary of RSA
*Encryption key (n, e) where $n = p \cdot q$ where p, q are primes *Encryption Function: $c = m$ mod m where m = block of letters in digit form $25 \cdot 25 \cdot 25 < n$ if digits = size of block

*Decryption Function
$e = m^{\bar{e} \mod n}$
e = inverse of $e \mod (p-1)(q-1)$

Example 7. Decrypt 09810461 with key(2537, 13)

1. $p = 43$, $q = 59$, $2537 = 43 \cdot 59$
2. $\bar{e} \cdot 13 \equiv 1 \mod 42 \cdot 58$
   $\bar{e} \cdot 13 \equiv 1 \mod 2436$
   $937 \cdot 13 - 5 \cdot 2436 = 1 \Rightarrow \bar{e} = 937$
3. $2525 < 2537 \rightarrow$ block size = 4
4. $m_1 = 0981$, $m_2 = 0461$
   $c_1 = m_1^{\bar{e}} \mod n \Rightarrow c_1 = 981^{937} \mod 2537 = 704$
   $c_2 = m_2^{\bar{e}} \mod n \Rightarrow c_2 = 461^{937} \mod 2537 = 1115$
5. 07041115 = HELP

*Note: RSA is considered a public cryptosystem because even though (n, e) is public, finding the prime factorization of n is impossible within a reasonable amount of time where n is very large.
RSA - 768 Case: n had 232 digits and it took several computers 2 years to find the factorization. If 1 computer had done it alone, it wouldve have taken 2,000 years.