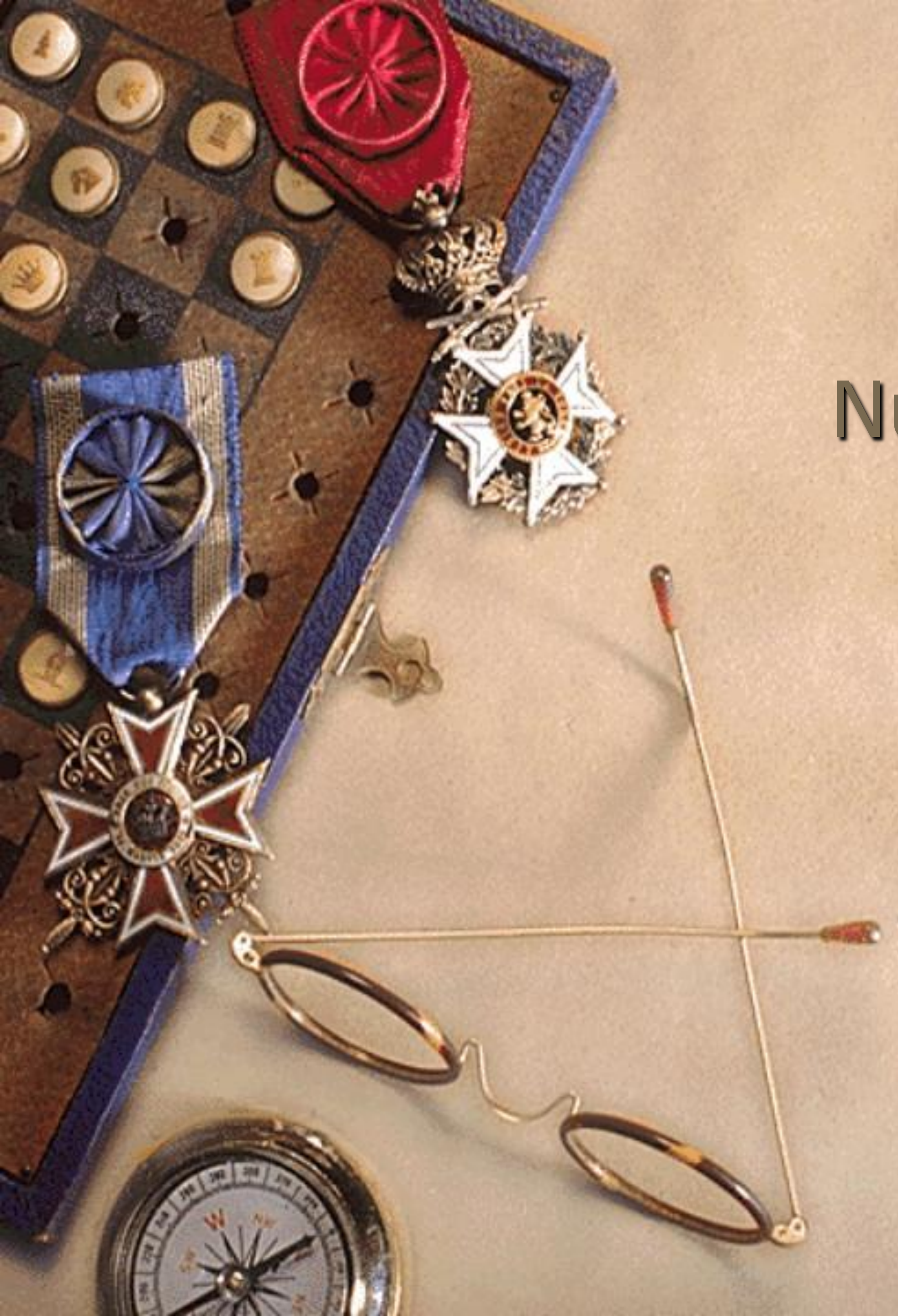

Number Theory and Cryptography

Chapter 4

Cryptography

Section 4.6

Section Summary

- Classical Cryptography
- Cryptosystems
- Public Key Cryptography
- RSA Cryptosystem
- Crytographic Protocols
- Primitive Roots and Discrete Logarithms

Caesar Cipher

B → E, X → 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 $\mathbf{Z}_{26}=\{0, 1,2,\ldots,25\}$
- The encryption function is $f(p) = (p + 3)$ **mod** 26.

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

Solution: 12 4 4 19   24 14 20   8 13   19 7 4   15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3)$ **mod** 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."

Caesar Cipher

- To recover the original message, use
  - $f^{-1}(p) = (p-3)$ **mod** 26.
- This process of recovering the original message from the encrypted message is called ***decryption***.

Shift Cipher

- 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

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

  and the decryption function is

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

  The integer k is called a *key*.

Example 1: Encrypt the message "STOP GLOBAL WARMING" using the shift cipher with $k = 11$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

18 19 14 15   6 11 14 1 0 11   22 0 17 12 8 13 6.

Apply the shift $f(p) = (p + 11) \textbf{ mod } 26$, 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."

Shift Cipher

Example 2: Decrypt the message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted using the shift cipher with $k = 7$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

11 4 22 11 24 15 11 20 9 11 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."

Affine Ciphers

- Shift ciphers are a special case of **affine ciphers** which use functions of the form

  $f(p) = (\mathbf{a}p + b)$ **mod** 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**: What letter replaces the letter K when the function $f(p) = (7p + 3)$ **mod** 26 is used for encryption.

  Solution: Since 10 represents K, $f(10) = (7\cdot10 + 3)$ **mod** 26 =21, which is then replaced by V.

Affine Ciphers

- 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 $\gcd(a,26) = 1$.
  - $\bar{a}(c - b) \equiv \bar{a}ap \pmod{26}$, which simplifies to $\bar{a}(c - b) \equiv p \pmod{26}$.
  - $p \equiv \bar{a}(c - b) \pmod{26}$ is used to determine p in $\mathbf{Z}_{26}$.

Cryptanalysis of Affine Ciphers

- The process of recovering plaintext from ciphertext without knowledge both of the encryption method and the key is known as *cryptanalysis* or *breaking codes*.
- An important tool for cryptanalyzing ciphertext produced with a affine ciphers is the relative frequencies of letters. The nine most common letters in the English texts are E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6%, and R 6%.
- To analyze ciphertext:
  - Find the frequency of the letters in the ciphertext.
  - Hypothesize that the most frequent letter is produced by encrypting E.
  - If the value of the shift from E to the most frequent letter is k, shift the ciphertext by $-k$ and see if it makes sense.
  - If not, try T as a hypothesis and continue.
- **Example**: We intercepted the message "ZNK KGXRE HOXJ MKZY ZNK CUXS" that we know was produced by a shift cipher. Let's try to cryptanalyze.
- **Solution**: The most common letter in the ciphertext is K. So perhaps the letters were shifted by 6 since this would then map E to K. Shifting the entire message by -6 gives us "THE EARLY BIRD GETS THE WORM."

Block Ciphers

- Ciphers that replace each letter of the alphabet by another letter are called *character* or **monoalphabetic** ciphers.
- They are vulnerable to cryptanalysis based on letter frequency. **Block ciphers** avoid this problem, by replacing blocks of letters with other blocks of letters.
- 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}.

Block Ciphers

Example: 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 encryted using the same cipher.

Solution:

a. Split into four blocks PIRA TEAT TACK.

Apply the permutation σ giving IAPR ETTA AKTC.

b. σ^{-1}: $\sigma^{-1}(1) = 2$, $\sigma^{-1}(2) = 4$, $\sigma^{-1}(3) = 1$, $\sigma^{-1}(4) = 3$.

Apply the permutation σ^{-1} giving USEW ATER HOSE.

Split into words to obtain USE WATER HOSE.

Cryptosystems

Definition: A *cryptosystem* is a five-tuple $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$, where

- $\mathcal{P}$ is the set of plainntext strings,
- $\mathcal{C}$ is the set of ciphertext strings,
- $\mathcal{K}$ is the *keyspace* (set of all possible keys),
- $\mathcal{E}$ is the set of encription functions, and
- $\mathcal{D}$ is the set of decryption functions.

- The encryption function in $\mathcal{E}$ corresponding to the key k is denoted by E_k and the decription function in $\mathcal{D}$ that decrypts cipher text enrypted using E_k is denoted by D_k. Therefore:

$$D_k(E_k(p)) = p, \text{ for all plaintext strings } p.$$

Cryptosystems

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

Solution: Assume the messages are strings consisting of elements in $\mathbf{Z}_{26}$.

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

Public Key Cryptography

- 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.

Clifford Cocks
(Born 1950)

The RSA Cryptosystem

- A public key cryptosystem, now known as the RSA system was introduced in 1976 by three researchers at MIT.

Ronald Rivest
(Born 1948)

Adi Shamir
(Born 1952)

Leonard Adelman(Born 1945)

- 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.

RSA Encryption

- **KEY GENERATION:**
  - Choose two distinct prime numbers p and q, say, with 200 digits each.
  - **Simple Example:** $p = 61$ and $q = 53$
  - Compute $n = pq$.
  - **Simple Example:** $n = 3233$
  - Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$.
  - **Simple Example:** $\varphi(n) = 3120$
  - Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
  - **Simple Example:** $e= 17$
  - Determine d as $d \equiv e-1 \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$) [This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$]
  - **Simple Example:**
    - $d = 2753$
    - Worked example for the modular multiplicative inverse
    - $d \times e \bmod \varphi(n) =1$
    - $2753 \times 17 \bmod 3120 =1$

RSA Encryption

- The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret.
- **Simple Example:** The public key is (e = 17) and the private key is (n = 3233, d = 2753).

RSA Encryption

Example: 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: 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 $C = M^{13}$ **mod** 2537.
- Since 1819^{13} mod $2537 = 2081$ and 1415^{13} mod $2537 = 2182$, the encrypted message is 2081 2182

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** $p \cdot q$. (*see text for full derivation*)

RSA Decryption

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

Solution: The message was encrypted with $n = 43\cdot 59$ and exponent 13. An inverse of 13 modulo $42\cdot 58 = 2436$ (*exercise* 2 *in Section* 4.4) 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.

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 protcol** is described by example.
  i. Suppose that Alice and Bob want to share a common key.
  ii. Alice and Bob agree to use a prime p and a primitive root a of p.
  iii. Alice chooses a secret integer k_1 and sends a^{k1} **mod** p to Bob.
  iv. Bob chooses a secret integer k_2 and sends a^{k2} **mod** p to Alice.
  v. Alice computes $(a^{k2})^{k1}$ **mod** p.
  vi. Bob computes $(a^{k1})^{k2}$ **mod** p.

At the end of the protocol, Alice and Bob have their shared key

$$(a^{k2})^{k1} \ \mathbf{mod}\ p = (a^{k1})^{k2} \ \mathbf{mod}\ p.$$

Cryptographic Protocols: Key Exchange

- To find the secret information from the public information would require the adversary to find k_1 and k_2 from a^{k1} **mod** p and a^{k2} **mod** p respectively. This is an instance of the discrete logarithm problem, considered to be computationally infeasible when p and a are sufficiently large.

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 $E_{(n,e)}(x) = x^d$ **mod** n. She decrypts a ciphertext message y using $D_{(n,e)}(y) = y^d$ **mod** 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 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.

Cryptographic Protocols: Digital Signatures

Example: Suppose Alice's RSA cryptosystem is the same as in the earlier example with key(2537,13), $2537 = 43 \cdot 59$, $p = 43$ and $q = 59$ are primes and $\gcd(e,(p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$.

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: Alice translates the message into blocks of digits 1204 0419 0019 1314 1413.

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

Query???

$$\sqrt{1+\sqrt{2+\sqrt{3+\sqrt{4\ldots.}}}}$$

$$\exists_{x\in\Re}\exists_{y\in\Re}(x = y) = ?$$

$$\sum_{x=1}^{\infty} x = ?$$

$$\sum_{x=1}^{\infty}\frac{1}{x} = ?$$

$$\forall_x(\Re \mid x) = ?$$

$$\exists_{x\in\Re}\exists_{y\in\Re}(x = y) = ?$$

$$\sqrt{1+\sqrt{2+\sqrt{3+\sqrt{4\ldots.}}}} = ?$$

$$1-1+1-1+1\ldots\ldots\ldots = ?$$

$$\sum_{x=1}^{\infty}\frac{1}{x} = ?$$