Chapter 1
Computer Security

Dr. Ahmad Al-Sabhany

1

Reference

- Understanding Cryptography A Textbook for Students and Practitioners, by Christof Paar and Jan Pelzl

2

Outline

- Introduction to Cryptology and Data Security
- Overview
- Symmetric Cryptology
- Simple Symmetric Encryption
- Cryptanalysis Overview
- Modular Arithmetic
- Historical Ciphers
- Stream Ciphers vs Bock Ciphers

3

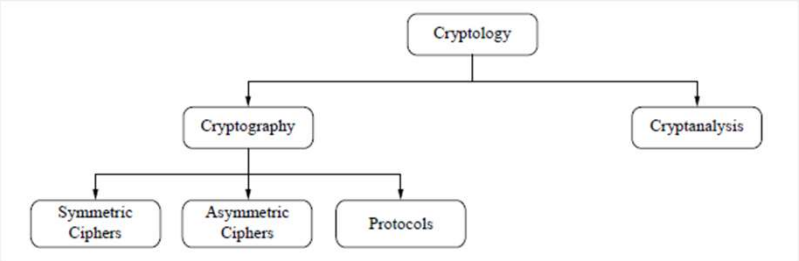
Introduction

- Cryptography started 200 B.C. in the Egyptian hieroglyphics
- Note the German Enigma encryption machine and the scytale of Sparta

- Cryptology vs. Cryptography
- Cryptography is the science of secret writing with the goal of hiding the meaning of a message.
- Cryptanalysis is the science and sometimes art of breaking cryptosystems.
  - cryptanalysis is the only way to assure that a cryptosystem is secure, it is an integral part of cryptology.
- Cryptology is the general term that includes, Cryptography and Cryptanalysis

4

Cryptology Overview

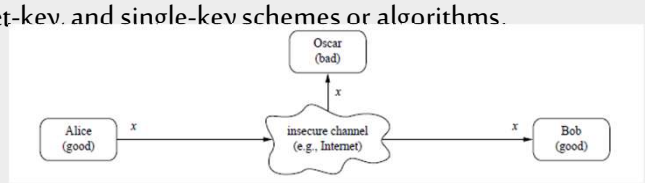


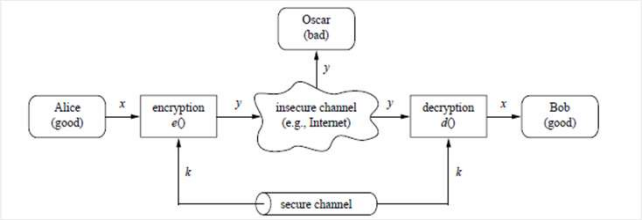
- Symmetric Algorithms: same key for encryption and decryption (Caesar, DES, AES).
- Asymmetric (or Public-Key) Algorithms: two keys, the public key for encryption, and the private key decryption (Diffie Helman, RSA, DSA).
- Cryptographic Protocols deals with application of cryptographic algorithms (TLS)

5

Symmetric Cryptography

- Also known as symmetric-key, secret-key, and single-key schemes or algorithms.
- x is called plaintext or cleartext,
- y is called ciphertext,
- k is called the key,
- the set of all possible keys is called the key space.





6

Simple Symmetric Encryption: The Substitution Cipher

- The substitution or the (= replacement) cipher.
- The goal of the substitution cipher is the encryption of text
- The idea is very simple: We substitute each letter of the alphabet with another one.
- Example 1.1.
  - A ⟶ k
  - B ⟶ d
  - C ⟶ w
- For instance, the pop group ABBA would be encrypted as kddk.

- It is not secure at all, and in the next slides we will look at way of attacking this cipher.

7

First Attack: Brute-Force or Exhaustive Key Search

- In this attack, the attacker simply decrypts the ciphertext with all possible keys.
- The attacker goal is the key for this cipher is which is the substitution table.

  Definition 1.2.1 Basic Exhaustive Key Search or Brute-force Attack Let (x,y) denote the pair of plaintext and ciphertext, and let K = {k1, ...,kK } be the key space of all possible keys ki. A brute-force attack now checks for every $k_i \in K$ if

  $$D_{k_i}(y) ?= x.$$

  If the equality holds, a possible correct key is found; if not, proceed with the next key.
- key space of the substitution cipher = $26 \cdot 25 \cdot \cdot \cdot 3 \cdot 2 \cdot 1 = 26! \approx 2^{88}$
- Even with hundreds of thousands of high-end PCs such a search would take several decades! Thus, we are tempted to conclude that the substitution cipher is secure. But this is incorrect because there is another, more powerful attack.
- brute-force attack from above treats the cipher as a black box

8

Second Attack: Letter Frequency Analysis (Statistical)

- The substitution cipher can easily be broken by such an analytical attack. The major weakness of the cipher is that each plaintext symbol always maps to the same ciphertext symbol. That means that the statistical properties of the plaintext are preserved in the ciphertext.
- Target: iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb hcc hwwhbsqvqbre hwq vhlq

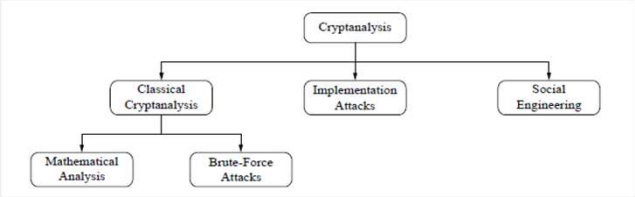
1. Determine the frequency of every ciphertext letter. The frequency distribution, often even of relatively short pieces of encrypted text, will be close to that of the given language in general. In particular, the most frequent letters can often easily be spotted in ciphertexts.
2. The method above can be generalized by looking at pairs or triples, or quadruples, and so on of ciphertext symbols.
   If we assume that word separators (blanks) have been found (which is only sometimes
3. the case), one can often detect frequent short words such as THE, AND, etc.

Letter Frequency Analysis (Statistical Attack)

- Note that the substitution table is the key of this cryptosystem.
- As always in symmetric cryptography, the key has to be distributed between Alice and Bob in a secure fashion.
- IQ IFCC VQQR FB RDQ VFLLCQ NA RDQ CFJWHWZ HR BNNB HCC HWWHBSQVQBRE HWQ VHLQ
- WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON ALL ARRANGEMENTS ARE MADE
- Good ciphers should hide the statistical properties of the encrypted plaintext. The ciphertext symbols should appear to be random.
- Also, a large key space alone is not sufficient for a strong encryption function.

Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0906
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007

Cryptanalysis Overview



- Classical Cryptanalysis: the science of recovering the plaintext x from the ciphertext y, or, alternatively, recovering the key k from the ciphertext y.
- Implementation Attacks: Side-channel analysis can be used to obtain a secret key, for instance, by measuring the electrical power consumption of a processor which operates on the secret key.
- Social Engineering Attacks: Bribing, blackmailing, tricking or classical espionage can be used to obtain a secret key by involving humans.

Kerckhoffs' Principle & Key Length

- Kerckhoffs' Principle : A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.
- ***How Many Key Bits Are Enough?***
  - The discussion of key lengths for symmetric crypto algorithms is only relevant if a brute-force attack is the best known attack.
  - The key lengths for symmetric and asymmetric algorithms are dramatically different. For instance, an 80-bit symmetric key provides roughly the same security as a 1024-bit RSA (RSA is a popular asymmetric algorithm) key.

Key length	Security estimation
56–64 bits	short term: a few hours or days
112–128 bits	long term: several decades in the absence of quantum computers
256 bits	long term: several decades, even with quantum computers that run the currently known quantum computing algorithms

Modular Arithmetic

- Almost all crypto algorithms, both symmetric ciphers and asymmetric ciphers, are based on arithmetic within a finite number of elements.
- Example 1.4. Consider the hours on a clock. If you keep adding one hour, you obtain: 1h,2h,3h, . . . ,11h,12h,1h,2h,3h, . . . ,11h,12h,1h,2h,3h, . . .

Definition 1.4.1 Modulo Operation
Let a, r,m $\in \mathbb{Z}$ *(where* $\mathbb{Z}$ *is a set of all integers) and* $m > 0$. *We write*

$$a \equiv r \bmod m$$

if m divides a−r.
m is called the modulus *and r is called the* remainder.

13

Modular Arithmetic

- Ex: a= 41, m=9
  41 = 4 * 9 + 5 ➔ r = 5
  check def. 1.4.1 (41-5) = 36, 9 | 36 ✓
- But also
  41 = 3.9 + 14 ➔ r = 14
  check def. 1.4.1 (41-15) = 27, 9 | 27 ✓
- But also
  42 = 5.9 + (-4) ➔ r = - 4
  check def. 1.4.1 (41+4) = 45, 9 | 45 ✓
- **The remainder is not unique**

14

Modular Arithmetic A - Equivalence Classes

- Ex: a = 12, m = 5

  $12 \equiv 2 \bmod 5$ check 5 | (12-2)

  $12 \equiv 7 \bmod 5$ check 5 | (12-7)

  $12 \equiv -3 \bmod 5$ check 5 | (12-(-3))

  $12 \equiv 17 \bmod 5$ check 5 | (12 - 17)

Def. the set

{ ..., -8, -3, 2, 7, 12, 17, ...}

forms an equivalence class modulo 5, all members of the class behaves equivalent modulo 5.

15

Modular Arithmetic A - Equivalence Classes

- Other classes equivalence Modulo. 5
  - I. {...-10,-5,0,5,10,15 ...}
  - II. {... -9,-4,1,6,11,16 ...}
  - III. {... -8,-3,2,7,12,17 ...}
  - IV. {... -7,-2,3,8,13,18 ...}
  - V. {... -6,-1,4,9,14,19 ...}

- Ex: Compute $(13.16 - 8 \bmod 5)$

  $13.16-8 = 208 - 8 = 200 \equiv 0 \bmod 5$

  ➔ $3 . 1 - 3 = 3-3 \equiv 0 \bmod 5$

  ➔ $8 . 6 - (-7) = 48 + 7 = 55 \equiv 0 \bmod 5$

- Ex: $3^8 \bmod 7 = ???$

  Bad way ➔ $3^8 = 6561 \equiv 2 \bmod 7$

  Using the Eqv. Classes ➔

  ➔ $3^8 = 3^4 . 3^4 = 81 . 81 = 4. 4 = 16 \equiv 2 \bmod 7$

  ➔ $3^8 = 3^2 . 3^2 . 3^2 . 3^2 = 9 . 9 . 9 . 9$

  $= 2 . 2 . 2. 2 = 16 \equiv 2 \bmod 7$

- Try computing $4^{14} \bmod 3$

16

Modular Arithmetic B – Rings _____Book Page 16 – 17

An algebraic view on Modular Arithmetic -

Definition 1.4.2 Ring

The integer ring $\mathbb{Z}_m$ *consists of:*

1. *The set* $\mathbb{Z}_m = \{0,1,2,\ldots,m-1\}$
2. *Two operations "+" and "×" for all* $a,b \in \mathbb{Z}m$ *such that:*
   i. $a+b \equiv c \bmod m$, $(c \in \mathbb{Z}_m)$
   ii. $a \times b \equiv d \bmod m$, $(d \in \mathbb{Z}_m)$

- Properties of rings
- We can add and multiply any two numbers and the result is always in the ring. A ring is said to be *closed*.
- Addition and multiplication are *associative*, e.g., $a+(b+c) = (a+b)+c$, and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a,b,c \in \mathbb{Z}_m$.

Modular Arithmetic B – Properties of rings

An algebraic view on Modular Arithmetic

- There is the *neutral element 0 with respect to addition*, i.e., for every element $a \in \mathbb{Z}_m$ it holds that $a+0 \equiv a \bmod m$.
- For any element a in the ring, there is always the negative element $-a$ such that $a+(-a) \equiv 0 \bmod m$, i.e., the *additive inverse* always exists.
  Ex: $3+(-3)=3+2=5\equiv 0 (\text{mod} 5)$.
- There is the *neutral element 1 with respect to multiplication*, i.e., for every element $a \in \mathbb{Z}_m$ it holds that $a \times 1 \equiv a \bmod m$.
- The *multiplicative inverse* exists only for some, but not for all, elements. Let $a \in \mathbb{Z}$, the inverse a^{-1} is defined such that

$$a \cdot a^{-1} \equiv 1 \bmod m$$

If an inverse exists for a, we can divide by this element since $b/a \equiv b \cdot a^{-1} \bmod m$.

Ring: Multiplicative Inverse Example

- For multiplicative inverses
  m = 9, Z_9 = {0,1,2,3,4,5,6,7,8}
  i. a = 2 find a^{-1}
  rule ➔ $a \cdot a^{-1} \equiv 1 \bmod 9$
  $2 \cdot 5 \equiv 1 \bmod 9$
  $a^{-1} \equiv 5 \bmod 9$
  ii. a = 6 find a^{-1}
  $6 \cdot \_\_\_ \equiv 5 \bmod 9$
  gcd(6,9) = 3 ≠ 1
- Rule If gcd (a,m) ≠ 1, the inverse does not exist

Shift Cipher (Caesar Cipher)

Definition 1.4.3 Shift Cipher
Let $x,y,k \in Z_{26}$.
Encryption: $e_k(x) \equiv x+k \bmod 26$.
Decryption: $d_k(y) \equiv y-k \bmod 26$.

- Example 1.11. Let the key be k = 17, and the plaintext is:
  ATTACK = x1,x2, . . . ,x6 = 0,19,19,0,2,10.
- The ciphertext is then computed as
  y1,y2, . . . ,y6 = 17,10,10,17,19,1 = rkkrtb
- #K = 26
- What is the best attack vector?

Affine Cipher

Definition 1.4.4 Affine Cipher
Let $x,y,a,b \in Z_{26}$
Encryption*:* $e_k(x) = y \equiv a \cdot x+b \bmod 26$.
Decryption*:* $d_k(y) = x \equiv a^{-1} \cdot (y-b) \bmod 26$.
with the key: $k = (a,b)$*, which has the restriction:* $\gcd(a,26) = 1$.

- The decryption is easily derived from the encryption function:
  $a \cdot x+b \equiv y \bmod 26$
  $a \cdot x \equiv (y-b) \bmod 26$
  $x \equiv a^{-1} \cdot (y-b) \bmod 26$

Affine Cipher

- The restriction $\gcd(a,26) = 1$ stems from the fact that the key parameter a needs to be inverted for decryption. We recall from Sect. 1.4.2 that an element a and the modulus must be relatively prime for the inverse of a to exist. Thus, a must be in the set:
  - $a \in \{1,3,5,7,9,11,15,17,19,21,23,25\}$ (1.2)
- But how do we find a^{-1}? For now, we can simply compute it by trial and error: For a given a we simply try all possible values a^{-1} until we obtain:
  - $a \cdot a^{-1} \equiv 1 \bmod 26$
- For instance, if $a = 3$, then $a^{-1} = 9$ since $3 \cdot 9 = 27 \equiv 1 \bmod 26$. Note that a^{-1} also always fulfills the condition $\gcd(a^{-1},26) = 1$ since the inverse of a^{-1} always exists.
- In fact, the inverse of a^{-1} is a itself. Hence, for the trial-and-error determination of a^{-1} one only has to check the values given in Eq. (1.2).

Affine Cipher

- *Example 1.12.* Let the key be $k = (a,b) = (9,13)$, and the plaintext be ATTACK = $x1,x2,\ldots,x6 = 0,19,19,0,2,10$.
- The inverse $a-1$ of a exists and is given by $a-1 = 3$. The ciphertext is computed as $y1,y2,\ldots,y6 = 13,2,2,13,5,25$ = nccnfz
- Is the affine cipher secure? No! The key space is only a bit larger than in the case of the shift cipher:
  #K key space = (#values for a)$\times$(#values for b) = $12 \times 26 = 312$
- What is the best attack vector for the Affine cipher?

23

Dr. Ahmad Al-Sabhany
alsabhany@uoa.edu.iq

24