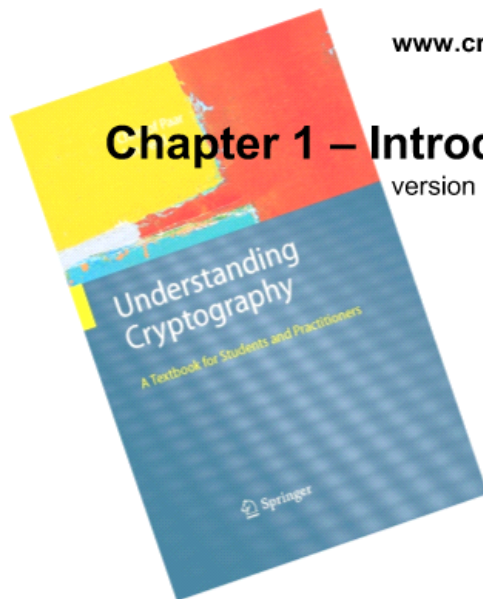




# Understanding Cryptography – A Textbook for Students and Practitioners

by Christof Paar and Jan Pelzl

[www.crypto-textbook.com](http://www.crypto-textbook.com)



## Chapter 1 – Introduction to Cryptography

version September 20, 2021

These slides were prepared by Christof Paar and Jan Pelzl, with minor modifications by Alwen Tiu, with the original authors' permission.

## Some legal stuff (sorry): Terms of Use

- The slides can be used free of charge. All copyrights for the slides remain with Christof Paar and Jan Pelzl.
- The title of the accompanying book “Understanding Cryptography” by Springer and the author’s names must remain on each slide.
- If the slides are modified, appropriate credits to the book authors and the book title must remain within the slides.
- It is not permitted to reproduce parts or all of the slides in printed form whatsoever without written consent by the authors.

## Content of this Chapter

- Overview on the field of cryptology
- Basics of symmetric cryptography
- Cryptanalysis
- Substitution Cipher
- Modular arithmetic
- Shift (or Caesar) Cipher and Affine Cipher

3/36

## Content of this Chapter

- **Overview on the field of cryptology**
- Basics of symmetric cryptography
- Cryptanalysis
- Substitution Cipher
- Modular arithmetic
- Shift (or Caesar) Cipher and Affine Cipher

4/36

## ■ Further Reading and Information

### Errata List for *Understanding Cryptography*.

- See [https://www.crypto-textbook.com/errata\\_list.php](https://www.crypto-textbook.com/errata_list.php)

### Addition to *Understanding Cryptography* .

- A.Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, October 1996.
- H.v.Tilborg (ed.), *Encyclopedia of Cryptography and Security*, Springer, 2005

### History of Cryptography (great bedtime reading)

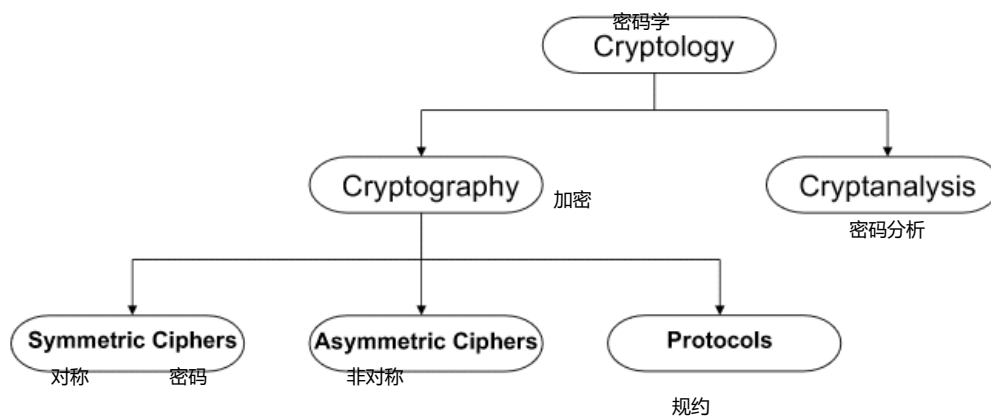
- S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor, 2000.
- D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. 2nd edition, Scribner, 1996.

### Software (excellent demonstration of many ancient and modern ciphers)

- CyberChef, <https://gchq.github.io/CyberChef/>
- JCryptool, <https://www.cryptool.org/en/jcryptool>

5/36

## ■ Classification of the Field of Cryptology



6/36

## ■ Some Basic Facts

- **Ancient Crypto:** Early signs of encryption in Egypt in ca. 2000 B.C.  
Letter-based encryption schemes (e.g., Caesar cipher) popular ever since.
- **Symmetric ciphers:** All encryption schemes from ancient times until 1976 were symmetric ones.
- **Asymmetric ciphers:** In 1976 public-key (or asymmetric) cryptography was openly proposed by Diffie, Hellman and Merkle.
- **Hybrid Schemes:** The majority of today's protocols are hybrid schemes, i.e., the use both
  - symmetric ciphers (e.g., for encryption and message authentication) and
  - asymmetric ciphers (e.g., for key exchange and digital signature).

7/36

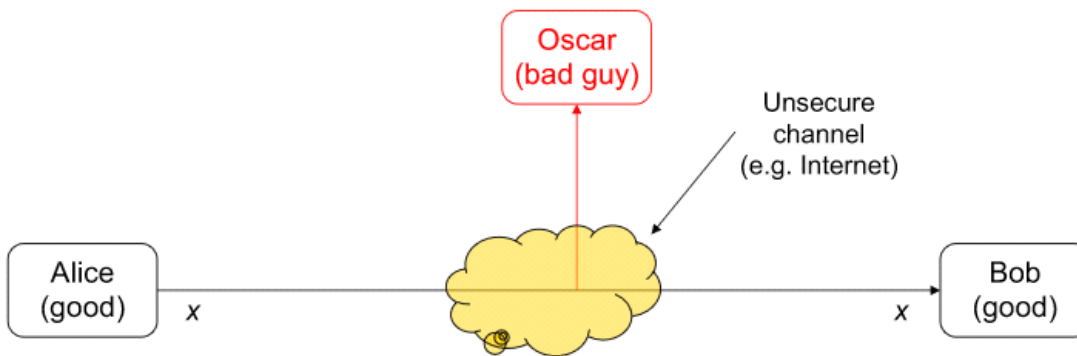
## Content of this Chapter

- Overview on the field of cryptology
- **Basics of symmetric cryptography**
- Cryptanalysis
- Substitution Cipher
- Modular arithmetic
- Shift (or Caesar) Cipher and Affine Cipher

8/36

## ■ Symmetric Cryptography 对称密码学

- Alternative names: **private-key**, **single-key** or **secret-key** cryptography.



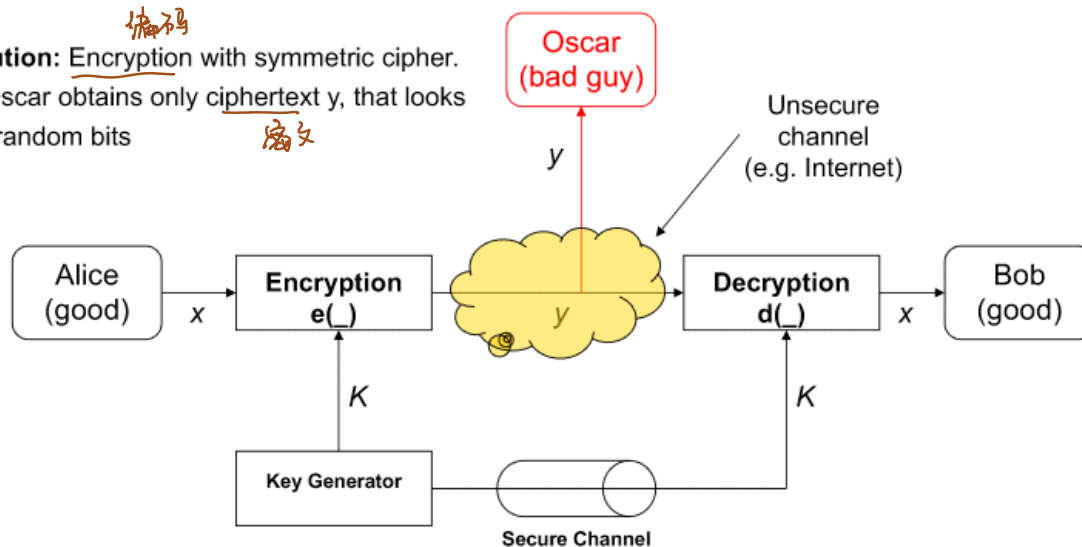
### • Problem Statement:

- 1) Alice and Bob would like to communicate via an unsecure channel (e.g., WLAN or Internet).
- 2) A malicious third party Oscar (the bad guy) has channel access but should not be able to understand the communication.

9/36

## ■ Symmetric Cryptography

**Solution:** Encryption with symmetric cipher.  
 ⇒ Oscar obtains only ciphertext  $y$ , that looks like random bits



- $x$  is the **plaintext** 明文
- $y$  is the **ciphertext** 密文
- $K$  is the **key**
- Set of all keys  $\{K_1, K_2, \dots, K_n\}$  is the **key space**

10/36

## ■ Symmetric Cryptography

- |                       |              |
|-----------------------|--------------|
| • Encryption equation | $y = e_K(x)$ |
| • Decryption equation | $x = d_K(y)$ |

- Encryption and decryption are inverse operations if the same key  $K$  is used on both sides:

$$d_K(y) = d_K(e_K(x)) = x$$

- **Important:** The key must be transmitted via a **secure channel** between Alice and Bob.
  - The secure channel can be realized, e.g., by manually installing the key for the Wi-Fi Protected Access (WPA) protocol or a human courier.
  - However, the system is only secure if an attacker does not learn the key  $K$ !
- ⇒ **The problem of secure communication is reduced to secure transmission and storage of the key  $K$ .**

11/36

## Content of this Chapter

- Overview on the field of cryptology
- Basics of symmetric cryptography
- **Cryptanalysis**
- Substitution Cipher
- Modular arithmetic
- Shift (or Caesar) Cipher and Affine Cipher

12/36

## ■ Why do we need Cryptanalysis?

- There is no *unconditional mathematical proof of security* for any practical cipher.
- One way to have a high assurance that a cipher is secure is to try to break it (and fail)!

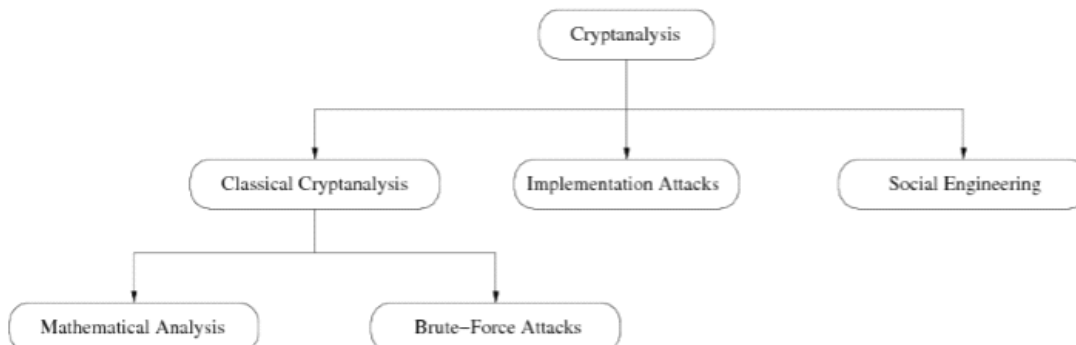
**Kerckhoff's Principle** is paramount in modern cryptography:

A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key.

- In order to achieve Kerckhoff's Principle in practice:  
**Only use widely known ciphers that have been cryptanalyzed for several years by good cryptographers!** (*Understanding Cryptography* only treats such ciphers)
- **Remark:** It is tempting to assume that a cipher is "more secure" if its details are kept secret. However, history has shown time and again that secret ciphers can almost always been broken once they have been reversed engineered. (Example: Content Scrambling System (CSS) for DVD content protection.)

13/36

## ■ Cryptanalysis: Attacking Cryptosystems



- **Classical Attacks**
  - Mathematical Analysis
  - Brute-Force Attack
- **Implementation Attack:** Try to extract key through reverse engineering or power measurement, e.g., for a banking smart card.
- **Social Engineering:** E.g., trick a user into giving up their password

14/36

## ■ Brute-Force Attack (or Exhaustive Key Search) against Symmetric Ciphers

- Treats the cipher as a black box 密钥长度决定了暴力破解的难度
- Requires (at least) 1 plaintext-ciphertext pair  $(x_0, y_0)$
- Check all possible keys until condition is fulfilled:  

$$d_K(y_0) \stackrel{?}{=} x_0$$
- How many keys to we need ?

Key length in bit	Key space	Security life time (assuming brute-force as best possible attack)
64	$2^{64}$	<b>Short term</b> (few days or less)
128	$2^{128}$	<b>Long-term</b> (several decades in the absence of quantum computers)
256	$2^{256}$	<b>Long-term</b> (also resistant against quantum computers – note that QC do not exist at the moment and might never exist)

Important: An adversary only needs to succeed with **one** attack. Thus, a long key space does not help if other attacks (e.g., social engineering) are possible..

15/36

## Content of this Chapter

- Overview on the field of cryptology
- Basics of symmetric cryptography
- Cryptanalysis
- **Substitution Cipher**
- Modular arithmetic
- Shift (or Caesar) Cipher and Affine Cipher

16/36



## ■ Substitution Cipher

- Historical cipher
- Great tool for understanding brute-force vs. analytical attacks
- Encrypts letters rather than bits (like all ciphers until after WW II)

**加密方式:** 通过替换明文中的每个字母为另一个固定字母来实现

**Idea: replace each plaintext letter by a fixed other letter.**

Plaintext		Ciphertext
A	→	k
B	→	d
C	→	w
....		

for instance, ABBA would be encrypted as kddk

- Example (ciphertext):

iq ifcc vqqr fb rdq vfllecq na rdq cfjwhwz hr bnnb hcc  
hwwhbsqvqbrc hwq vhlq

- How secure is the Substitution Cipher? Let's look at attacks...

17/36

## ■ Attacks against the Substitution Cipher

### Exhaustive Key Search (Brute-Force Attack)

- Simply try every possible substitution table until an intelligent plaintext appears (note that each substitution table is a key)..

- How many substitution tables (= keys) are there?

26 个字母可以有  $26 \times 25 \times \dots \times 1 = 26!$  种排列组合。

$$26 \times 25 \times \dots \times 3 \times 2 \times 1 = 26! \approx 2^{88}$$

**Search through  $2^{88}$  keys is completely infeasible with today's computers!**

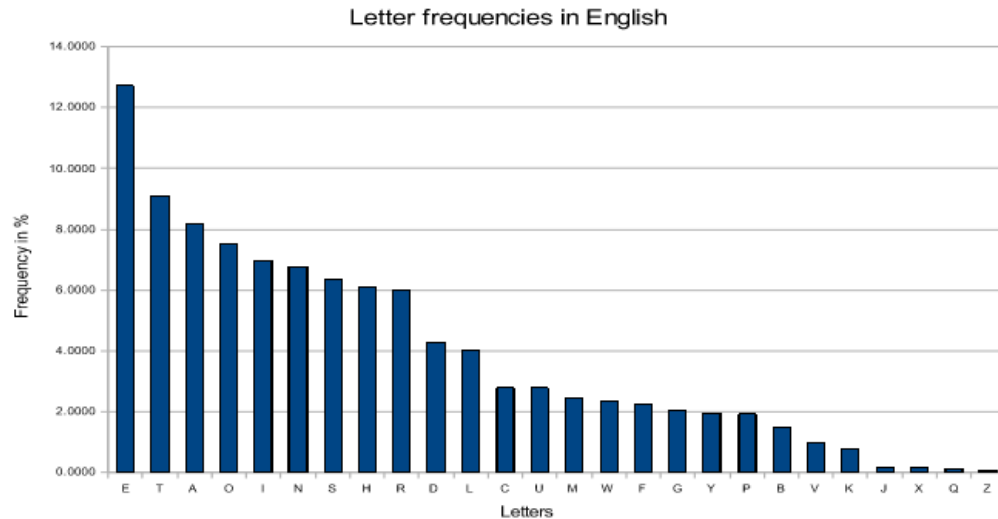
(cf. earlier table on key lengths)

- Q: Can we now conclude that the substitution cipher is secure since a brute-force attack is not feasible?
- A: No! We have to protect against **all** possible attacks...

18/36

## ■ Letter Frequency Analysis (Brute-Force Attack)

- Letters have very different frequencies in the English language
- Moreover: the frequency of plaintext letters is preserved in the ciphertext.
- For instance, "e" is the most common letter in English; almost 13% of all letters in a typical English text are "e".
- The next most common one is "t" with about 9%.



19/36

## ■ Breaking the Substitution Cipher with Letter Frequency Attack

- Let's return to our example and identify the **most frequent letter**:

```
i q ifcc v q q r fb rd q v f l l c q na rd q cfjwhwz hr bnnb hcc  
hwwhbs q v q bre hw q vhl q
```

- We replace the ciphertext **letter q** by **E** and obtain:

```
i E ifcc v E E r fb rd E v f l l c E na rd E cfjwhwz hr bnnb hcc  
hwwhbs E v E bre hw E vhl E
```

- By further guessing based on the frequency of the remaining letters we obtain the plaintext:

```
WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON ALL  
ARRANGEMENTS ARE MADE
```

20/36

## ■ Breaking the Substitution Cipher with Letter Frequency Attack

- In practice, not only frequencies of individual letters can be used for an attack, but also the frequency of letter pairs (i.e., „th“ is very common in English), letter triples, etc.
- cf. Problem 1.1 in *Understanding Cryptography* for a longer ciphertext you can try to break!

**Important lesson:** Even though the substitution cipher has a sufficiently large key space of appr.  $2^{88}$ , it can easily be defeated with analytical methods. This is an excellent example that an encryption scheme must withstand all types of attacks.

21/36

## Content of this Chapter

- Overview on the field of cryptology
- Basics of symmetric cryptography
- Attacking crypto schemes
- Substitution Cipher
- **Modular arithmetic**
- Shift (or Caesar) Cipher and Affine Cipher

22/36

## ■ Short Introduction to Modular Arithmetic

### Why do we need to study modular arithmetic?

- Extremely important for asymmetric cryptography (RSA, elliptic curves etc.)
- Some historical ciphers can be elegantly described with modular arithmetic (cf. Caesar and affine cipher later on).

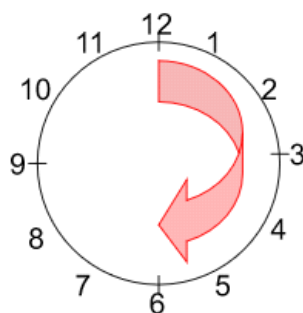
23/36

## ■ Short Introduction to Modular Arithmetic

Generally speaking, most cryptosystems are based on **sets of numbers** that are

1. **discrete** (sets with integers are particularly useful)
2. **finite** (i.e., if we only compute with a finitely many numbers)

Seems too abstract? --- Let's look at a finite set with discrete numbers we are quite familiar with: a clock.



Interestingly, even though the numbers are incremented every hour we never leave the set of integers:

1, 2, 3, ... 11, 12, 1, 2, 3, ... 11, 12, 1, 2, 3, ...:

24/36

## ■ Short Introduction to Modular Arithmetic

- We develop now an arithmetic system which allows us to **compute** in finite sets of integers like the 12 integers we find on a clock (1,2,3, ... ,12).
- It is crucial to have an operation which "keeps the numbers within limits", i.e., after addition and multiplication they should never leave the set (i.e., never larger than 12).

### Definition: Modulus Operation

Let  $a, r, m$  be integers and  $m > 0$ . We write

$$a \equiv r \bmod m$$

if  $(a - r)$  is divisible by  $m$ .

- $m$  is called the **modulus**
- $r$  is called the **remainder**

Examples for modular reduction.

- Let  $a = 12$  and  $m = 9$  :  $12 \equiv 3 \bmod 9$
- Let  $a = 34$  and  $m = 9$ :  $34 \equiv 7 \bmod 9$
- Let  $a = -7$  and  $m = 9$ :  $-7 \equiv 2 \bmod 9$

(you should check whether the condition " $m$  divides  $(a-r)$ " holds in each of the 3 cases)

25/36

## ■ Properties of Modular Arithmetic (1)

- **The remainder is not unique**

It is somewhat surprising that for every given modulus  $m$  and number  $a$ , there are (infinitely) many valid remainders.

Example:

- $12 \equiv 3 \bmod 9$   $\rightarrow$  3 is a valid remainder since 9 divides  $(12 - 3)$
- $12 \equiv 21 \bmod 9$   $\rightarrow$  21 is a valid remainder since 9 divides  $(12 - 21)$
- $12 \equiv -6 \bmod 9$   $\rightarrow$  -6 is a valid remainder since 9 divides  $(12 - (-6))$

26/36

## ■ Properties of Modular Arithmetic (2)

- Which remainder do we choose?

By convention, we usually agree on the **smallest non-negative integer  $r$**  as remainder. This integer can be computed as

$$a = \overset{\text{quotient}}{q} \times m + \overset{\text{remainder}}{r} \quad \text{where } 0 \leq r \leq m - 1$$

- Example:  $a=12$  and  $m=9$

$$12 = 1 \times 9 + 3 \quad \rightarrow r = 3$$

Remark: This is just a convention. Algorithmically we are free to choose any other valid remainder to compute our crypto functions.

27/36

## ■ Properties of Modular Arithmetic (3)

- How do we perform modular division?

First, note that rather than performing a division, we **prefer to multiply by the inverse**. Ex:

$$\frac{b}{a} \equiv b \times a^{-1} \pmod{m}$$

The inverse  $a^{-1}$  of a number  $a$  is defined such that:

$$a a^{-1} \equiv 1 \pmod{m}$$

Ex: What is  $\frac{5}{7} \pmod{9}$ ?

The inverse of  $7 \pmod{9}$  is 4 since  $7 \times 4 \equiv 28 \equiv 1 \pmod{9}$ , hence:

$$\frac{5}{7} \equiv 5 \times 4 = 20 \equiv 2 \pmod{9}$$

- How is the inverse computed?

The inverse of a number  $a \pmod{m}$  only exists if and only if:

$$\gcd(a, m) = 1$$

(note that in the example above  $\gcd(5, 9) = 1$ , so that the inverse of 5 exists modulo 9)

Here we use an exhaustive search to compute the inverse. A more efficient method uses the Euclidean Algorithm (see Chapter 6 of *Understanding Cryptography*).

28/36

## ■ Properties of Modular Arithmetic (4)

- **Modular reduction can be performed at any point during a calculation**

Let's look first at an example. We want to compute  $3^8 \bmod 7$  (note that exponentiation is extremely important in public-key cryptography).

### 1. Approach: Exponentiation followed by modular reduction

$$3^8 = 6561 \equiv 2 \bmod 7$$

Note that we have the intermediate result 6561 even though we know that the final result can't be larger than 6.

### 2. Approach: Exponentiation with intermediate modular reduction

$$3^8 = 3^4 3^4 = 81 \times 81$$

At this point we reduce the intermediate results 81 modulo 7:

$$3^8 = 81 \times 81 \equiv 4 \times 4 \bmod 7$$

$$4 \times 4 = 16 \equiv 2 \bmod 7$$

Note that we can perform all these multiplications without pocket calculator, whereas mentally computing  $3^8 = 6561$  is a bit challenging for most of us.

**General rule: For most algorithms it is advantageous to reduce intermediate results as soon as possible.**

29/36

## ■ An Algebraic View on Modulo Arithmetic: The Ring $Z_m$ (1)

We can view modular arithmetic in terms of sets and operations in the set. By doing arithmetic modulo  $m$  we obtain **the integer ring  $Z_m$**  with the following properties:

- **Closure:** We can add and multiply any two numbers and the result is always in the ring.
- Addition and multiplication are **associative**, i.e., for all  $a, b, c \in Z_m$   
$$a + (b + c) = (a + b) + c$$
$$a \times (b \times c) = (a \times b) \times c$$
and addition is **commutative**:  $a + b = b + a$
- The **distributive law** holds:  $a \times (b + c) = (a \times b) + (a \times c)$  for all  $a, b, c \in Z_m$ .
- There is the **neutral element 0 with respect to addition**, i.e., for all  $a \in Z_m$   
$$a + 0 \equiv a \bmod m$$
- For all  $a \in Z_m$ , there is always **an additive inverse element  $-a$**  such that  
$$a + (-a) \equiv 0 \bmod m$$
- There is the **neutral element 1 with respect to multiplication**, i.e., for all  $a \in Z_m$   
$$a \times 1 \equiv a \bmod m$$
- The **multiplicative inverse  $a^{-1}$**   
$$a \times a^{-1} \equiv 1 \bmod m$$
exists only for some, but not for all, **elements in  $Z_m$** .

30/36

## ■ An Algebraic View on Modulo Arithmetic: The Ring $Z_m$ (2)

Roughly speaking, a ring is a structure in which we can always add, subtract and multiply, but we can only divide by certain elements (namely by those for which a multiplicative inverse exists).

- We recall from above that an element  $a \in Z_m$  has a multiplicative inverse only if:

$$\gcd(a, m) = 1$$

We say that  $a$  is **coprime or relatively prime to  $m$** .

在整数环  $Z_m$  中, 一个元素  $a$  只有当它与  $m$  互素时, 才有乘法逆元

- Ex: We consider the ring  $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$   
The elements 0, 3, and 6 do not have inverses since they are not coprime to 9.  
The inverses of the other elements 1, 2, 4, 5, 7, and 8 are:

$$1^{-1} \equiv 1 \pmod{9}$$

$$2^{-1} \equiv 5 \pmod{9}$$

$$4^{-1} \equiv 7 \pmod{9}$$

$$5^{-1} \equiv 2 \pmod{9}$$

$$7^{-1} \equiv 4 \pmod{9}$$

$$8^{-1} \equiv 8 \pmod{9}$$

31/36

## Content of this Chapter

- Overview on the field of cryptology
- Basics of symmetric cryptography
- Attacking crypto schemes
- Substitution Cipher
- Modular arithmetic
- **Shift (or Caesar) Cipher and Affine Cipher**

32/36



## ■ Shift (or Caesar) Cipher (1)

凯撒密码

将每个明文字母替换为字母表中向后移动  $k$  位的字母

- Ancient cipher, allegedly used by Julius Caesar
- Replaces each plaintext letter by another one.
- Replacement rule is very simple: Take letter that follows after  $k$  positions in the alphabet

Needs mapping from letters  $\rightarrow$  numbers:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Example for  $k = 7$

Plaintext = ATTACK = 0, 19, 19, 0, 2, 10

Ciphertext = haa jr = 7, 0, 0, 7, 17

Note that the letters "wrap around" at the end of the alphabet, which can be mathematically be expressed as reduction modulo 26, e.g.,  $19 + 7 = 26 \equiv 0 \pmod{26}$

$$19 + 7 = 26 \equiv 0 \pmod{26}$$

33/36

## ■ Shift (or Caesar) Cipher (2)

- Elegant mathematical description of the cipher.

Let  $k, x, y \in \{0, 1, \dots, 25\}$

- Encryption:  $y = e_k(x) \equiv x + k \pmod{26}$
- Decryption:  $x = d_k(y) \equiv y - k \pmod{26}$

- Q: Is the shift cipher secure?
- A: **No!** several attacks are possible, including:
  - Exhaustive key search (key space is only 26)
  - Letter frequency analysis, similar to attack against substitution cipher
- **穷举密钥攻击**: 密钥空间仅为 26 个可能的值 (即  $k=0, 1, \dots, 25$ ), 非常容易被暴力破解。
- **字母频率分析**: 由于英文文本中某些字母 (如 e 和 t) 的出现频率较高, 通过分析密文中的字母频率可以快速推断出明文。

34/36

## ■ Affine Cipher

- Extension of the shift cipher: rather than just adding the key to the plaintext, we also multiply by the key
- We use for this a key consisting of two parts:  $k = (a, b)$

Let  $k, x, y \in \{0, 1, \dots, 25\}$

- Encryption:  $y = e_k(x) \equiv ax + b \pmod{26}$
- Decryption:  $x = d_k(y) \equiv a^{-1}(y - b) \pmod{26}$

- Since the inverse of  $a$  is needed for inversion, we can only use values for  $a$  for which:  
 $\gcd(a, 26) = 1$

There are 12 values for  $a$  that fulfill this condition.

- From this follows that the key space is only  $12 \times 26 = 312$  (cf. Sec 1.4 in *Understanding Cryptography*)
- Again, several attacks are possible, including:
  - Exhaustive key search and letter frequency analysis, similar to the attack against the substitution cipher

穷举攻击和字母频率分析攻击

35/36

## ■ Lessons Learned

- Never develop your own crypto algorithm unless you have a team of experienced cryptanalysts checking your design.
- Do not use unproven crypto algorithms or unproven protocols.
- Attackers always look for the weakest point of a cryptosystem. For instance, a large key space by itself is no guarantee for a cipher being secure; the cipher might still be vulnerable against analytical attacks.
- Key lengths for symmetric algorithms in order to thwart exhaustive key-search attacks:
  - 64 bit: insecure except for data with extremely short-term value
  - 128 bit: long-term security of several decades, unless quantum computers become available (quantum computers do not exist and perhaps never will)
  - 256 bit: as above, but probably secure against attacks by quantum computers.
- Modular arithmetic is a tool for expressing historical encryption schemes, such as the affine cipher, in a mathematically elegant way.

36/36