第二章

2.1 什么是对称密码的本质成分？

Plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.

明文 加密算法 密钥 密文 解密算法

2.2 密码算法中两个基本函数式什么？

Permutation and substitution.

代换和置换 P20

2.3 用密码进行通信的两个人需要多少密钥？

对称密码只需要一把，非对称密码要两把 P20

2.4 分组密码和流密码的区别是什么？

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

分组密码每次输入的一组元素，相应地输出一组元素。流密码则是连续地处理输入元素，每次输出一个元素。 P20

2.5 攻击密码的两种一般方法是什么？

Cryptanalysis and brute force.

密码分析和暴力破解

2.6 列出并简要定力基于攻击者所知道信息的密码分析攻击类型。

Ciphertext only . One possible attack under these circumstances is the brute-force approach of trying all possible keys. If the key space is very large, this becomes impractical. Thus, the opponent must rely on an analysis of the ciphertext itself, generally applying various statistical tests to it.

Known plaintext. The analyst may be able to capture one or more plaintext messages as well as their encryptions. With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed.

Chosen plaintext. If the analyst is able to choose the messages to encrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key.

惟密文

已知明文

选择明文

2.7 无条件安全密码和计算上安全密码的区别是什么？

An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. An encryption scheme is said to be computationally secure if: (1) the cost of breaking the cipher exceeds the value of the encrypted information, and (2) the time required to break the cipher exceeds the useful lifetime of the information.

书本 P21

2.8 简要定义 Caesar 密码

The Caesar cipher involves replacing each letter of the alphabet with the letter standing k places further down the alphabet, for k in the range 1 through 25.

书本 P22

2.9 简要定义单表代换密码

A monoalphabetic substitution cipher maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet.

书本 P23

2.10 简要定义 Playfair 密码

The Playfair algorithm is based on the use of a 5 ⨯ 5 matrix of letters constructed using a keyword. Plaintext is encrypted two letters at a time using this matrix.

书本 P26

2.11 单表代换密码和夺标代换密码的区别是什么？

A polyalphabetic substitution cipher uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.

书本 P30

2.12 一次一密的两个问题是什么？

1. There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.

2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

书本 P33

2.13 什么是置换密码？

A transposition cipher involves a permutation of the plaintext letters.

书本 P33

2.14 什么是隐写术？

Steganography involves concealing the existence of a message.

书本 P36

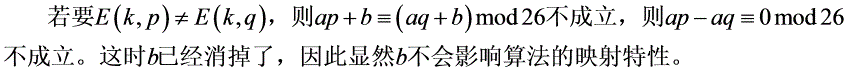
2.7.3 习题

2.1

a. 对 b 的取值是否有限制？解释原因。

没有限制， b 只会使得明文加密后的密文字母统一左移或右移，因此如果是单射的， b 改变后依然是单射。

注：答案解答得很坑爹，答了等于没答。现解答如下 :



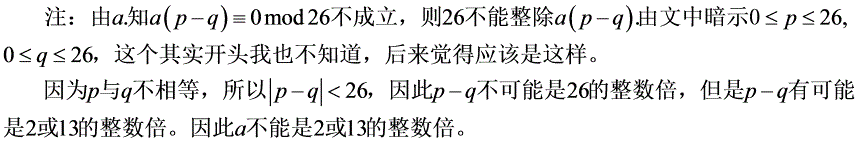
b. 判定 a 不能取哪些值。

2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24. 当 a 大于 25 时， a 也不能是使得 a mod 26 为这些数的值。

c. 分析 a 可以取那些值，不可以取那些值。并给出理由。

a 与 26 必须没有大于 1 的公因子。也就是说 a 与 26 互素，或者最大公约数为 1. 为了说明为什么是这样，先注意到要使 E( a , p ) = E( a , q ) (0 ≤ p ≤ q < 26) 成立当且仅当 26 整除 a ( p – q ) .

1. 假如 a 与 26 互素 . 则 26 不能整除 a ( p – q ) . 这是因为不能减小 a /26 的这部分而且 ( p – q ) 小于 26. 2. 假如 a 和 26 有公因子 k > 1 . 则当 q = p + m / k ≠ p 时， p – q = - m / k ，显然 26 能整除 a ( p – q ) ，从而 E( a , p ) = E( a , q ) .



2.2 有多少种仿射 Caesar 密码？

a 有 12 种可能的值（ 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24 ）， b 有 26 种可能的值（ 0 到 25 ），因此总共有 12 26 = 312 种仿射 Caesar 密码。

2.3 用仿射 Caesar 密码加密得到一份密文。频率最高的字母为 B ，次高的字母为 U ，请破译该密码。

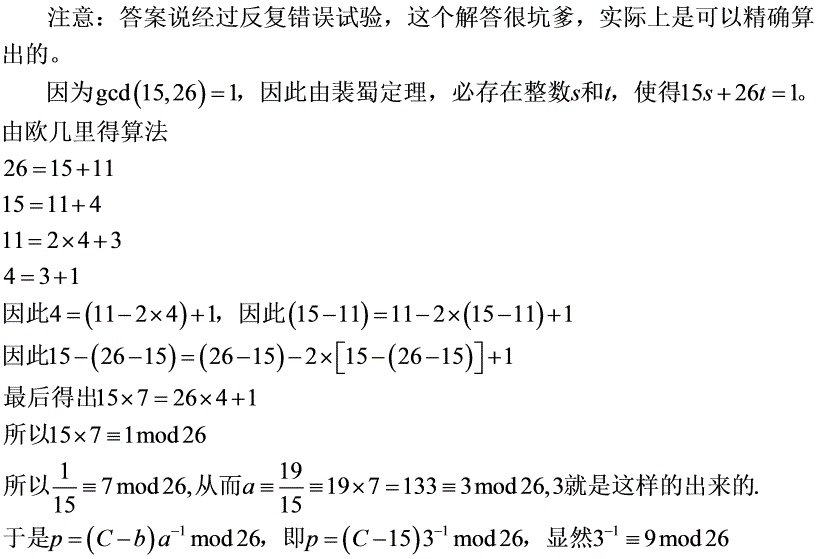
假设明文中频率最高的字母为 e ，次高的字母为 t 。注意 e=4 （ e 排在第 4 ， a 排在第 0 ，没有第 26 ）， B=1 ， t=19 ， U=20 ；因此可以得到：

1 = (4 a + b ) mod 26

20 = (19 a + b ) mod 26

下式减上式可得 19 = 15 a mod 26 ，通过反复的错误实验，可得 a = 3

然后代入第一条式子可得 1 = (12 + b ) mod 26 ，然后得出 b = 15



2.4 A good glass in the Bishop's hostel in the Devil's seat—twenty-one degrees and thirteen minutes—northeast and by north—main branch seventh limb east side—shoot from the left eye of the death's head— a bee line from the tree through the shot fifty feet out. (from The Gold Bug, by Edgar Allan Poe)

2.5

a. 第一个字母 t 对应 A ，第二个字母 h 对应 B ， e 对应 C ， s 对应 D ，依此类推。随后在句子中重复出现的字母则忽略。结果是

密文 : SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA

明文 : basilisk to leviathan blake is contact

b. 这是一个单表密码，因此容易被破译

c. 最后一句可能不会包含字母表中的所有字母。如果用第一句的话，随后的句子可以继续填补第一句字母的不全。

2.6 The cipher refers to the words in the page of a book. The first entry, 534, refers to page 534. The second entry, C2, refers to column two. The remaining numbers are words in that column. The names DOUGLAS and BIRLSTONE are simply words that do not appear on that page. Elementary! (from The Valley of Fear, by Sir Arthur Conan Doyle)

2.6 密文其实指的是一本书中某一页的单词。第一项， 534 是指第 534 页。第二项， C2 是指第二列。剩余的数字是这一列中的单词。名字 DOUGLAS 和 BIRLSTONE 显然是那一页没有出现的单词。太基本了！ (from The Valley of Fear, by Sir Arthur Conan Doyle)

2.7 a. 加密方法是 ，先把字母从左到右，从上到下填入矩阵中。然后按第一个密钥的编号，先把编号为 1 的那一列作为下一个矩阵的第一行，随后的编号按上面的方法填入对应的行。最后按第二个密钥的编号一列一列地写出来。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 8 | 10 | 7 | 9 | 6 | 3 | 1 | 4 | 5 |
| C | R | Y | P | T | O | G | A | H | I |
| B | E | A | T | T | H | E | T | H | I |
| R | D | P | I | L | L | A | R | F | R |
| O | M | T | H | E | L | E | F | T | O |
| U | T | S | I | D | E | T | H | E | L |
| Y | C | E | U | M | T | H | E | A | T |
| R | E | T | O | N | I | G | H | T | A |
| T | S | E | V | E | N | I | F | Y | O |
| U | A | R | E | D | I | S | T | R | U |
| S | T | F | U | L | B | R | I | N | G |
| T | W | O | F | R | I | E | N | D | S |
|  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | 2 | 8 | 10 | 5 | 6 | 3 | 7 | 1 | 9 |
| N | E | T | W | O | R | K | S | C | U |
| T | R | F | H | E | H | F | T | I | N |
| B | R | O | U | Y | R | T | U | S | T |
| E | A | E | T | H | G | I | S | R | E |
| H | F | T | E | A | T | Y | R | N | D |
| I | R | O | L | T | A | O | U | G | S |
| H | L | L | E | T | I | N | I | B | I |
| T | I | H | I | U | O | V | E | U | F |
| E | D | M | T | C | E | S | A | T | W |
| T | L | E | D | M | N | E | D | L | R |
| A | P | T | S | E | T | E | R | F | O |
|  |  |  |  |  |  |  |  |  |  |

ISRNG BUTLF RRAFR LIDLP FTIYO NVSEE TBEHI HTETA

EYHAT TUCME HRGTA IOENT TUSRU IEADR FOETO LHMET

NTEDS IFWRO HUTEL EITDS

b. 解密当然是把矩阵倒转顺序来用，先用第二个矩阵。首先，根据第二个密钥的编码，把密文按编码的顺序填入列中。然后，再用第一个密钥，从左到右，从上到下地读第二个矩阵，按照第一个密钥的编码顺序，把第一行的字母填入编码为 1 的列中，随后的行依此类推。最后，第一个矩阵从左到右从上到下读就是明文了。

c. 虽然这是一个弱的加密方法，但是当加密的内容是实时信息，或者企图窃听者没有快速得到好的密码分析方法（例如，战略使用），也是可以使用的。加上它除了纸和笔外不需要跟多的工具，而且非常容易记住。

2.8 SPUTNIK

2.9 PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION

2.10

a.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L | A | R | G | E |
| S | T | B | C | D |
| F | H | I/J | K | M |
| N | O | P | Q | U |
| V | W | X | Y | Z |
|  |  |  |  |  |

b.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| O | C | U | R | E |
| N | A | B | D | F |
| G | H | I/J | K | L |
| M | P | Q | S | T |
| V | W | X | Y | Z |
|  |  |  |  |  |

2.11

a. UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

b. UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

c. 轮换对称的行或者列会导致等价的结果。在这一例子中，通过一步的列轮换和三步的行轮换，此问题的 a 部分的矩阵可以从问题 2.10a 的矩阵得到。

2.12 a. 25! 2 84

b. 对于给定的任意 5x5 配置的矩阵，对于每一行，都有四个轮换变换（循环右移一格、两格、三格、四格）是等价的，总共就有五个是一样的。这五行之中，各自每一行也有这样的等价关系。所以每个配置就代表着 25 个等价的配置。因此，总共的密钥数量应为 25!/25 = 24!

2.13 一个混合的 Ceasar 密码。移位的数量由密钥决定，密钥决定矩阵中字母的代换。

2.14 a. Difficulties are things that show what men are.

b. Irrationally held truths may be more harmful than reasoned errors.

2.15

a.

我们需要偶数个字母，因此在最后添加一个 ”q” 。然后按照字母表的位置变换字母。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | e | e | t | m | e | a | t | t | h | e | u | s | u | a | l |
| 13 | 5 | 5 | 20 | 13 | 5 | 1 | 20 | 20 | 8 | 5 | 21 | 19 | 21 | 1 | 12 |
| P | l | a | c | e | a | t | t | e | n | r | a | t | h | e | r |
| 16 | 12 | 1 | 3 | 5 | 1 | 20 | 20 | 5 | 14 | 18 | 1 | 20 | 8 | 5 | 18 |
| T | h | a | n | e | i | g | h | t | o | c | l | o | c | k | q |
| 20 | 8 | 1 | 14 | 5 | 9 | 7 | 8 | 20 | 15 | 3 | 12 | 15 | 3 | 11 | 17 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

必须一次对两个字母进行计算，第一对是



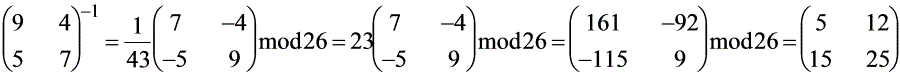
密文的头两个字符是字母表的第 7 和 22 个位置，对应 GV

完整的密文：

GVUIGVKODZYPUHEKJHUZWFZFWSJSDZMUDZMYCJQMFWWUQRKR

b.

我们首先求矩阵的逆。注意到加密矩阵的模是 (9 7) – (4 5) = 43 . 使用书中求逆矩阵的公式：



这里我们利用了等式 (43) –1 = 23 mod 26 。一旦逆矩阵确定，解密就能够顺利执行了。来源 : [LEWA00].

2.16

考虑矩阵 K ，由元素 k ij 表示，矩阵 K j 是矩阵 K 的第 j 列。

and

通过选择下列 n 组明文就能暴露出 K 矩阵的每一列 :

(B, A, A, …, A, A) ↔ K 1

(A, B, A, …, A, A) ↔ K 2

:

(A, A, A, …, A, B) ↔ K n

注意， A 代表 0 ， B 代表 1

2.17

2.17 a. 7 134

b. 7 134

c. 134

d. 10 134

e. 24 132

f. 24 (132 – 1) 13

g . 37648

h. 23530

i. 157248

2.18 密钥 : legleglegle

明文 : explanation

密文 : PBVWETLXOZR

2.19 a.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| s | e | n | d | m | o | r | e | m | o | n | e | y |
| 18 | 4 | 13 | 3 | 12 | 14 | 17 | 4 | 12 | 14 | 13 | 4 | 24 |
| 9 | 0 | 1 | 7 | 23 | 15 | 21 | 14 | 11 | 11 | 2 | 8 | 9 |
| 1 | 4 | 14 | 10 | 9 | 3 | 12 | 18 | 23 | 25 | 15 | 12 | 7 |
| B | E | C | K | J | D | M | S | X | Z | P | M | H |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

b.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| c | a | s | h | n | o | t | n | e | e | d | e | d |
| 2 | 0 | 18 | 7 | 13 | 14 | 19 | 13 | 4 | 4 | 3 | 4 | 3 |
| 25 | 4 | 22 | 3 | 22 | 15 | 19 | 5 | 19 | 21 | 12 | 8 | 4 |
| 1 | 4 | 14 | 10 | 9 | 3 | 12 | 18 | 23 | 25 | 15 | 12 | 7 |
| B | E | C | K | J | D | M | S | X | Z | P | M | H |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

2.20 your package ready Friday 21st room three Please destroy this immediately.

2.21

a. 把信息填入 8 列的矩阵总，每个整数告诉你应选择各行的第几个字母。结果 :

He sitteth between the cherubims. The isles may be glad thereof. As the rivers in the south.

b. 挺安全的，每一行是 1/8 的概率。因此如果密文长度是 8 的倍数，那么明文也可能是 8 的倍数。

c. 不是很安全， Lord Peter 就破解了它。 ( 出自 The Nine Tailors )