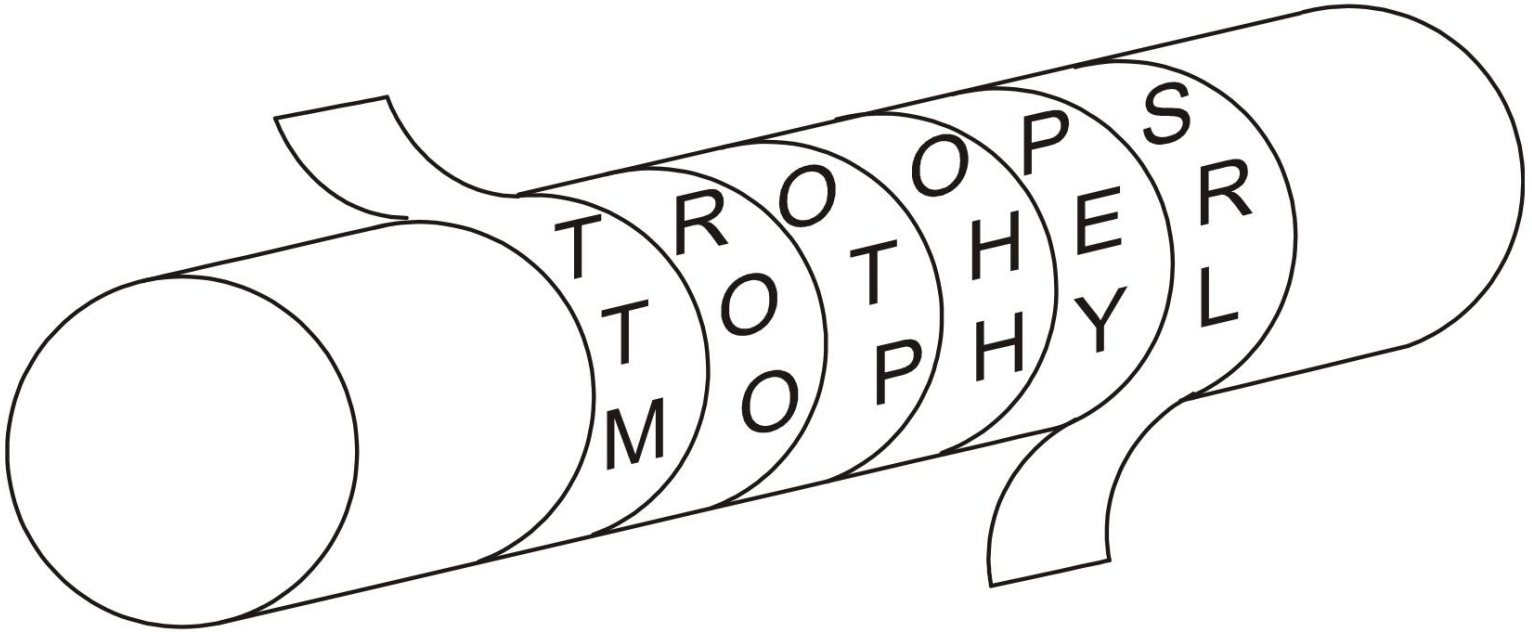
歷史程序

1. 賽塔萊
2. 凱撒
3. Vigenere 4. 謎

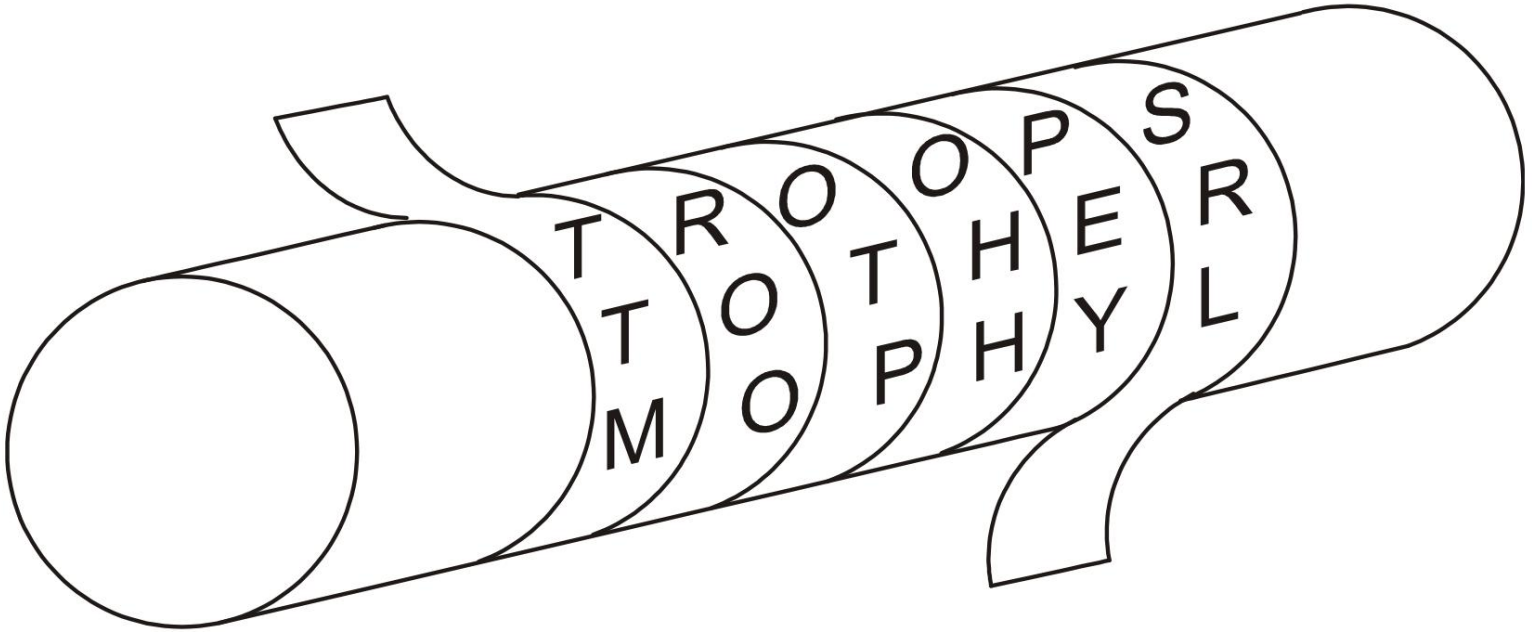
賽塔萊



換位密碼：位置在公元前 5 世紀發生了變化。斯巴達人
使用

轉置在現代密碼學方法中也很重要！

賽塔萊



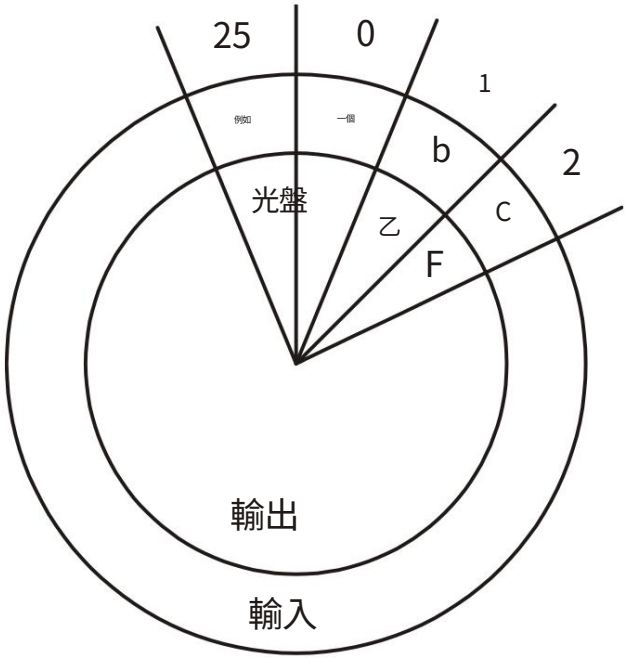
磁帶上有什麼？

TTMROOOTPOHHPEYSRL

關鍵是什麼？

桿的直徑。

單字母替換（凱撒）



純文本 :m

關鍵文本 :c

（字母編號 :BN）

關鍵 :凱撒的k = 3

a (0) D (3) b

(1) E (4) c (2)

F(5)

...

w (22) Z (25) x

(23) A (0) y (24)

B (1) z (25) C (2)

凱撒數學

移動 k 個位置（對於凱撒，k=3）

加密：BN $_C$ = (國陣 $_米$ + k) 模組 26

解密：BN $_米$ = (國陣 $_C$ - k) 模組 26

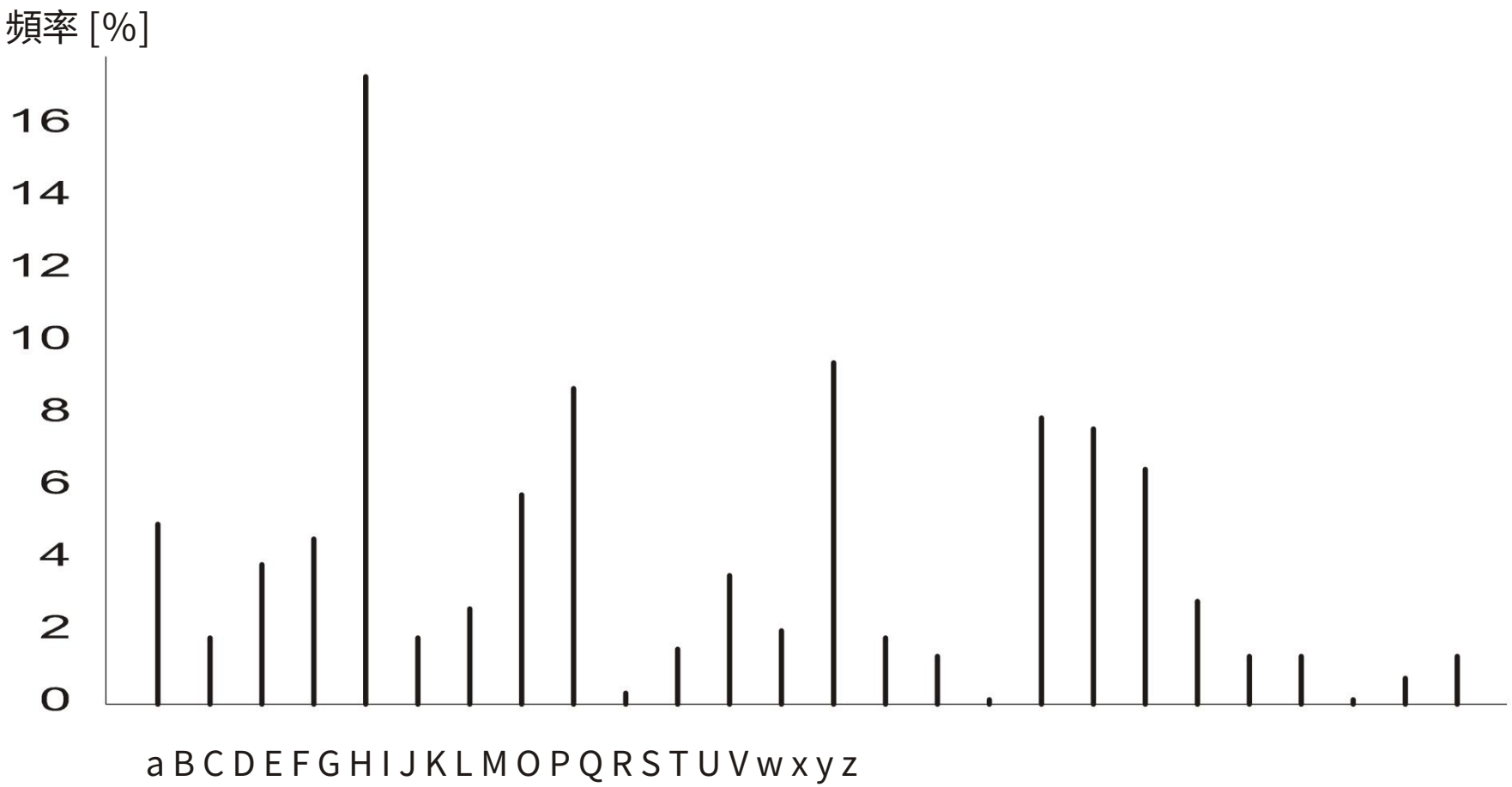
凱撒在一個團體〈 26, + mod 26 〉

替換密碼的安全性

- 凱撒 :鑰匙只有 26 種可能性
  程序必須保密 · 保密總是不好的（Kerckhoff 原則）

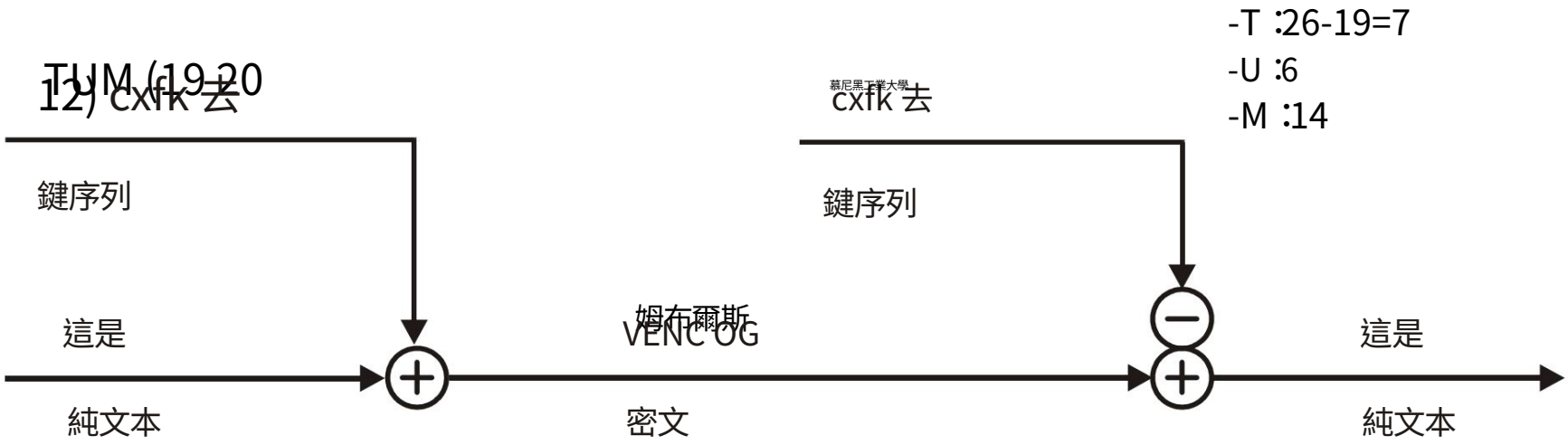
- 替換錶 :26 !可能的表 · 密鑰空間非常大 :大約 288 · 因此該方法是不可破壞的嗎？

頻率分析



單字母替換不會改變頻率分佈！

多字母替換 (Vigenère)



t M (19 + 19) mod 26 = 12

h B (7 + 20) mod 26 = i

U (8 + 12) mod 26 = s

L (18 + 19) mod 26 = i C

(8 + 20) mod 26 =

1

20

11

2

M t (12 + 7) mod 26 = 19

.....

Vigenère 加密的解密

- 卡西斯基測試

  1854 年，C. Babagge 解密了使用 Vigenère 方法加密的文本

  1863 FW Kasiski 發布程序

  程序：

  - 搜索字母序列的重複 - 測量重複之間的距離 - 距離的素數或倍數給出

  密鑰長度 h - 然後對 h 組字母進行頻率分析

示例 Kasiski 測試（維基百科）

資料來源 :http://de.wikipedia.org/wiki/Kasiski-Test

純文本變成了秘密文本

PLU TOPLUTOP盧托 PLU TOPLUTOPLU

SPL DZPCNXLI HCKR OFG ZSWPCFHTIN

你什麼都看不見。

純文本變成秘密文本

PLU TOPLUTOP LUTOP LUTOP LUTOP

SPL DZPCNXLI HYKRT RYASXXNXLI

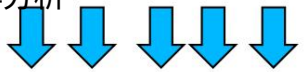
可以看到距離15 = 3*5

密鑰長度為 h=5

h 列

SPLDZ
PCNXL
IHCKR
OFGZS
世界和平基金會
錫

頻率分析



冥王星

德克
ARTEX
TWIRD
一起
家
分機

Vigenère 加密的解密

- W. Friedman 的弗里德曼測試 ,1925 年
  - 已知 :一種語言中字母的頻率分佈。
  - 由此確定字母對的重合指數 :κ
    7.62%（德語） ,κ e = 6.61%（英語）
  - 隨機字母序列的重合指數 :κr = 1/26 = 3.85%
  - 那麼長度為 n 的密文的重合指數 κ
    確實 。該指數包括：
    - 隨機序列（不等密鑰對）
    - 語言相關重合指數
      （具有相同密鑰的對）
  - 可以從文本的重合指數估計密鑰長度
    變為 :h ≈ (κd - κr) n / [(n-1) κ - κr n + κ d)]

IE =

Lehrstuhl für Sicherheit
in der Informationstechnik

費用德量檢驗的推導

）博士）n IE hn2

移位密碼的完美安全性

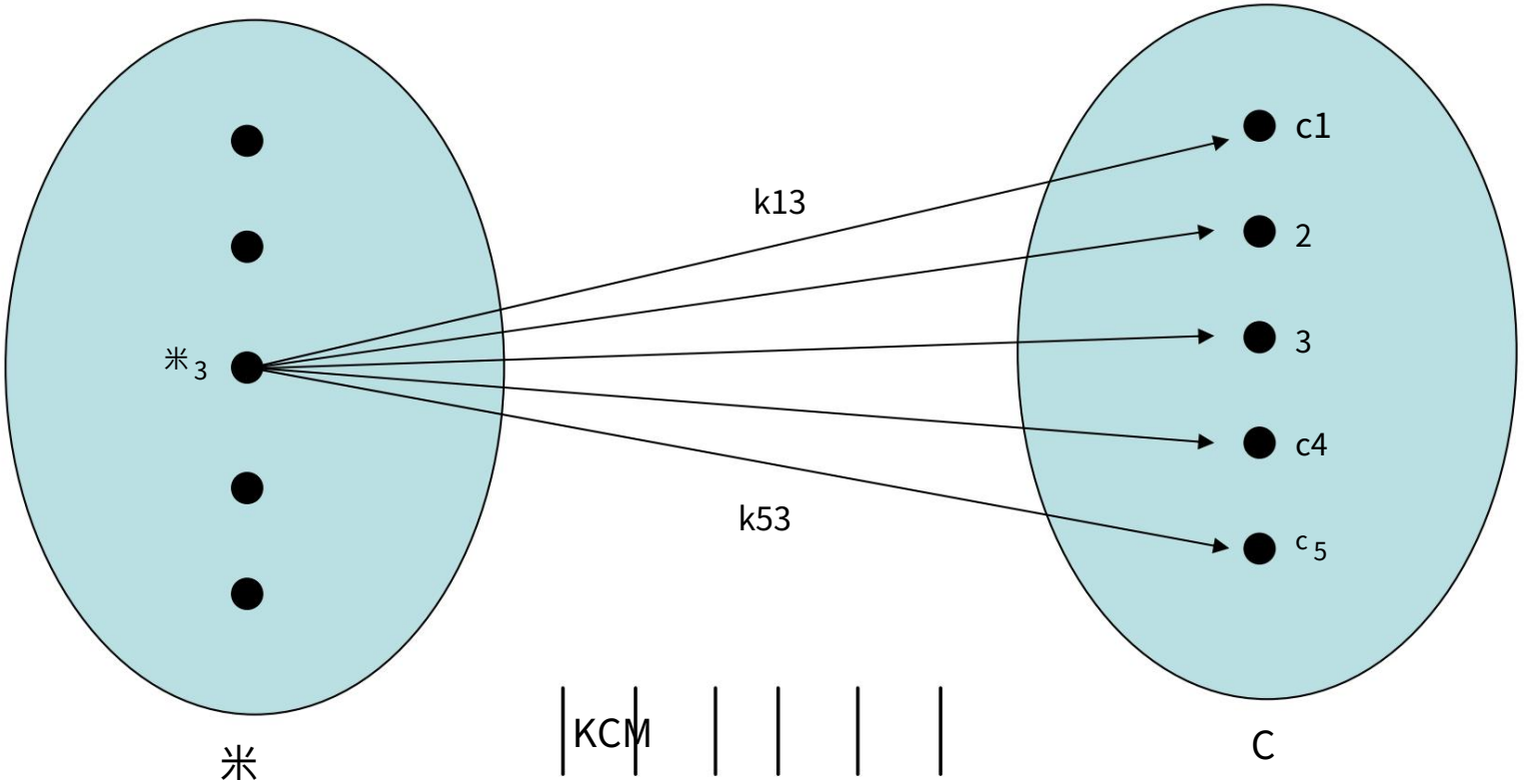
純文本 ,是哪一個？

從攻擊者收到的密碼

ci1 = (mj1 + kij1) mod 26

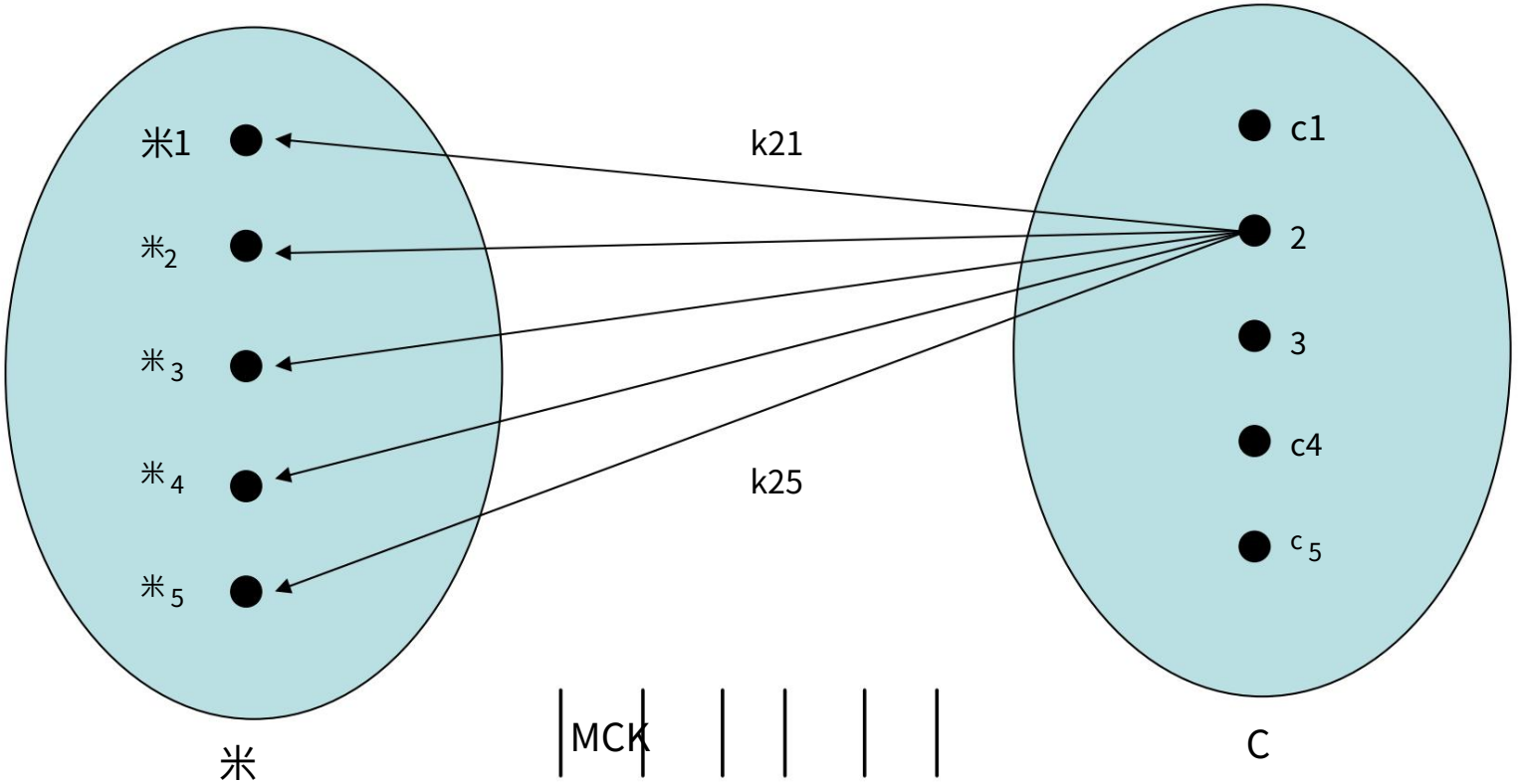
對於給定的密碼和任何假定的明文 ,可以構造一個密鑰序列！

完善的安全性



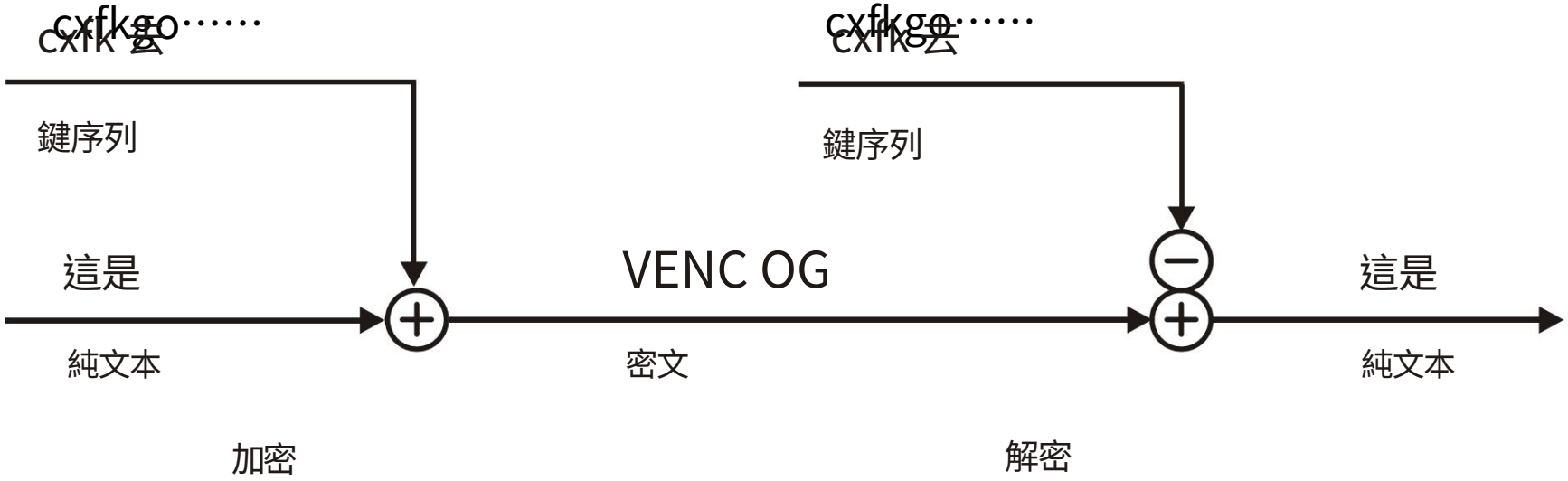
所有密鑰的可能性均等，因此每個密碼的可能性均等

完善的安全性



所有密鑰的可能性均等，因此每個明文的可能性均等

多表替換



鑰匙

- 無限長
- 使用一次
- 隨機生成

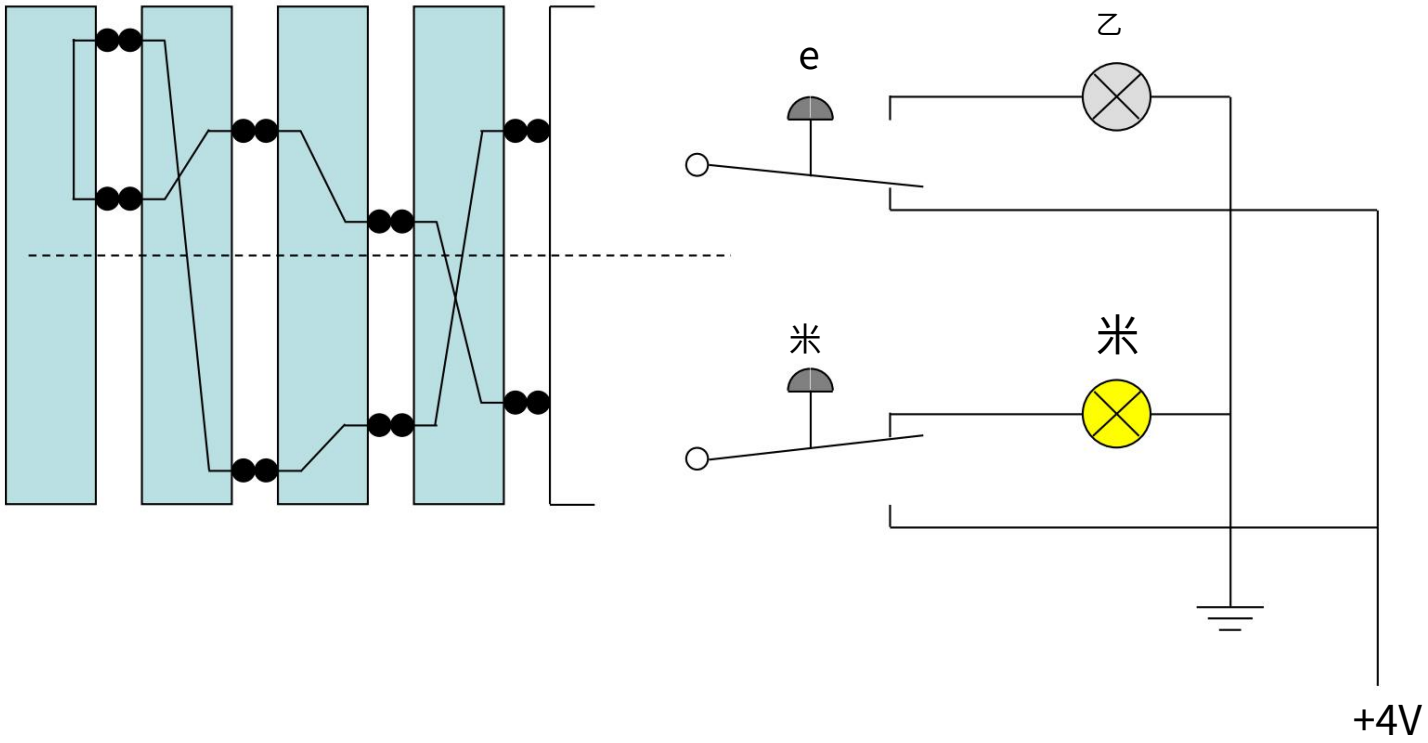
完善的安全性

問題：要求實現起來非常複雜！

加密機器 :例如 Enigma

Enigma :鍵序列示例

帶反轉盤的 3 轉子 Enigma 電路



cryptool 中的演示(http://www.cryptool.de/)

謎 :獨特的屬性

- 3 或 4 個轉子 ,每個轉子有 26 個位置 · 每

個轉子 ,位置相關的排列（輸入/輸出列表）

- 像公里計數器這樣的轉子每個字母都會前進一個位置
- 加密 :Enter -> 指示燈
- 3 個轉子 :26 3 個可能的位置
- 5 個捲軸中的 3 個 :60 種可能性
- 6 線麵包板 :6 對字母交換 26!/14!/6!/2 ^{6} = 1.0*1011
- 鑰匙： 轉子 、連接器的初始位置
- 解密 :相同的密鑰（對稱）

  開關/燈泡互換
- 通過嘗試 26 3 或 26 4 位置（鍵)來破解密碼
- 波蘭/英國密碼學家破壞的程序

密碼學的里程碑

軍事行動

- 公元前500 年。
  斯巴達人的 Scytale · 公元前 50 年。
  凱撒的替代密碼
- 855
  頻率分析是阿拉伯學者發明的
- 1590
  Vigenère改進的凱撒長期以來被認為是完美的
  看到加密
- 1854
  巴貝奇破解維熱內爾（1863 年卡西斯基獨立）
- 1883
  克爾霍夫原理
- 1917
  Mauborgne/Vernam 共同發明“One Time Pad”，可證明的完美安全性
- 1923
  謝爾比烏斯發明了謎
- ~1930
  Rejewski 破譯謎題
- ~1940
  圖靈造解碼機

密碼學的里程碑

工業用途

計算機和網絡

- 1974 年

  IBM (Feistel) 開發 DES 前身

- 1976 年

  Diffie/Hellmann 解決密鑰分配問題

- 1977 年

  Rivest、Shamir、Adleman 發明了第一個非對稱密碼學算法

適合所有人的密碼學

- 1990

  齊默爾曼首先發表 PGP的發布

- 2009

  英特爾集成了硬件加速器和特殊他的 AES 說明處理器

密碼學的應用

- 自古以來：軍事情報 g
- 從 1970 年開始：工業數據傳輸 (DES)
- 從 1980 年開始：移動通信（GSM、芯片卡）
- 自 1990 年以來：日常使用（例如 PGP、WLAN、TPM）

示例芯片卡 - 適合所有人的安全硬件：

- 電信：電話卡、SIM 卡
- 支付功能：借記卡、信用卡
- 訪問控制：訪問通行證、票證
- 國民身份證：護照、駕照、健康卡
- 數字版權管理：付費電視、藍光