现代密码学

第三讲 外国古代密码艺术

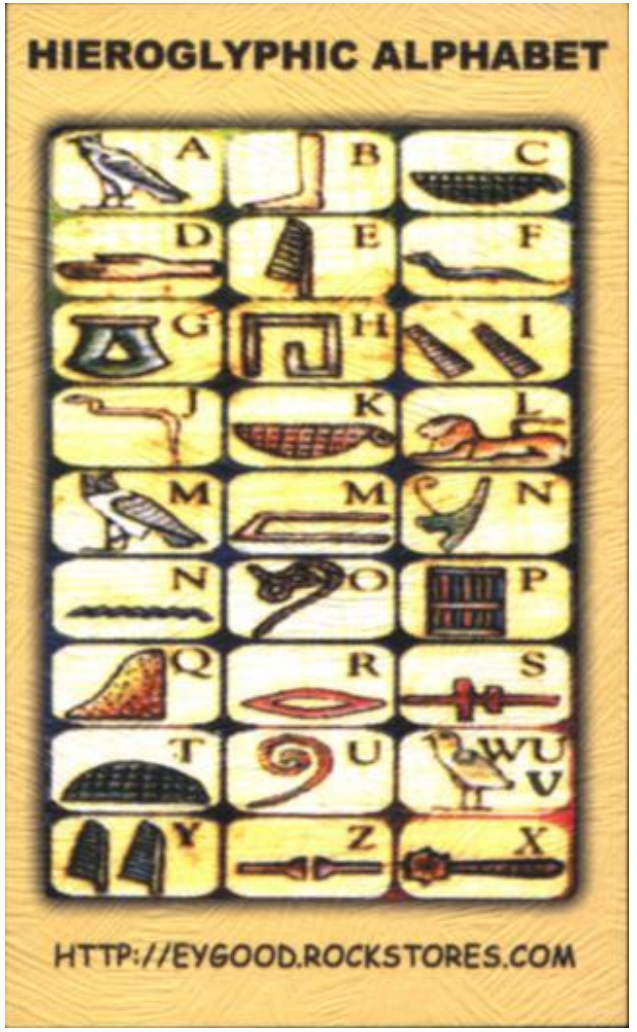
信息与软件工程学院

第三讲 外国古代密码艺术

- 代替密码
- 换位密码
- 密码机

密码学的起源

- 象形文字的修改：密码学的第一个例子是对标准书写符号的修改，例如古埃及法老坟墓上的文字（3200-1100 B.C.），核心思想是代替(Substitution)



棋盘密码

- 205-123 B.C.，古希腊人棋盘密码

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

HELLO → 2315313134

兽栏法

明文：System

密文： 

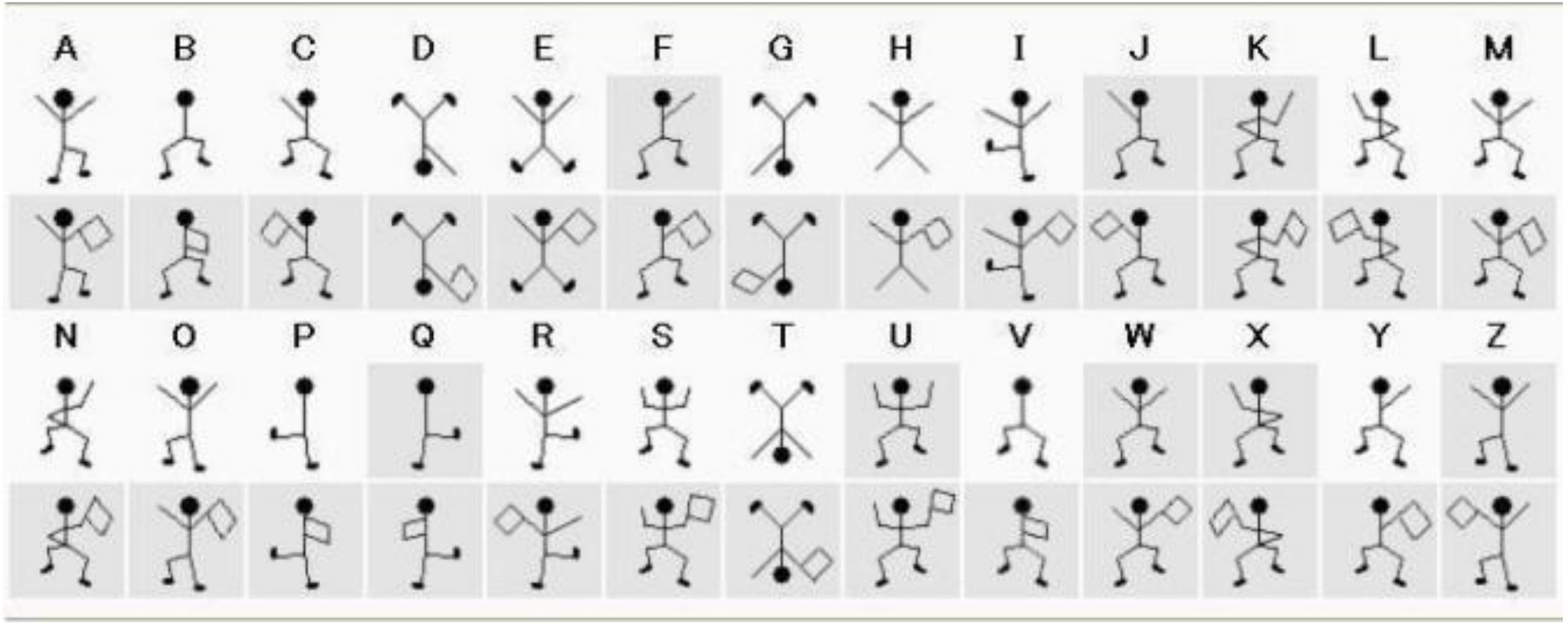
密文字母表（需要保密）：

A	B	C
D	E	F
G	H	I

J.	K.	.L
M.	N.	.O
P.	Q.	.R

S:	T:	:U
V:	W:	:X
Y:	Z:	:.

跳舞的小人



摩尔斯密码

摩 尔 斯 电 码 表

字符	电码符号	字符	电码符号	字符	电码符号
A	• —	N	— •	1	• — — — —
B	— • • •	O	— — —	2	• • — — —
C	— • — •	P	• — — •	3	• • • — —
D	— • •	Q	— — • —	4	• • • • —
E	•	R	• — •	5	• • • • •
F	• • — •	S	• • •	6	— • • • •
G	— — •	T	—	7	— — • • •
H	• • • •	U	• • —	8	— — — • •
I	• •	V	• • • —	9	— — — — •
J	• — — —	W	• — —	0	— — — — —
K	— • —	X	— • • —	?	• • — — • •
L	• — • •	Y	— • — —	/	— • • — •
M	— —	Z	— — • •	( )	— • — — • —
				—	— • • • • —
				•	• — • — • —

恺撒密码

- 50 B.C.，古罗马恺撒密码（移位密码或加法密码）

A	B	C	D	E	F	G	……	X	Y	Z
D	E	F	G	H	I	J	……	A	B	C

HELLO → KHOOR

1593年， 推广为**Vigenère**密码——分组加法密码

第三讲 外国古代密码艺术

- 代替密码
- 换位密码
- 密码机

报文倒置

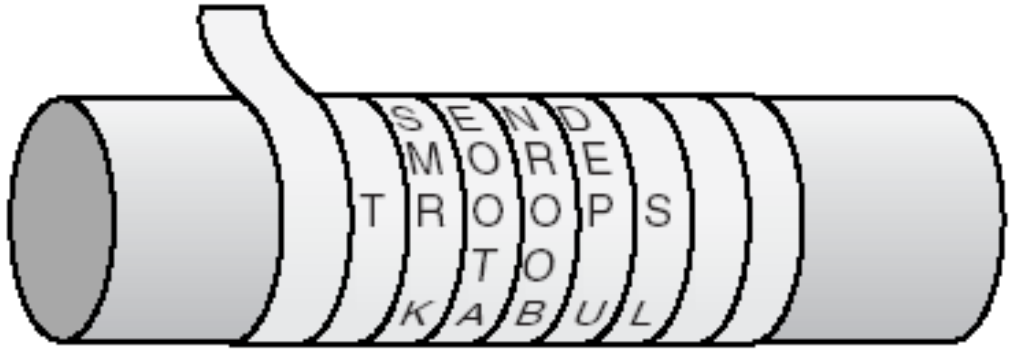
明文：never accept failure no matter how often it visits you

密文：uoys tisi vtin etfo wohr etta mone ulia ftpe ccar even

特点：简单，缺点是不安全，很容易被识破。

Scytale密码（天书）

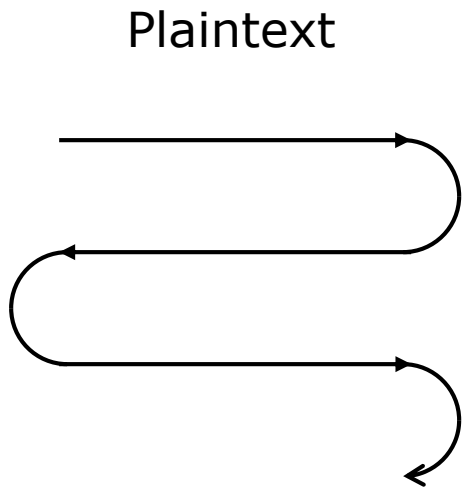
500 B.C.，古斯巴达人使用的“天书”

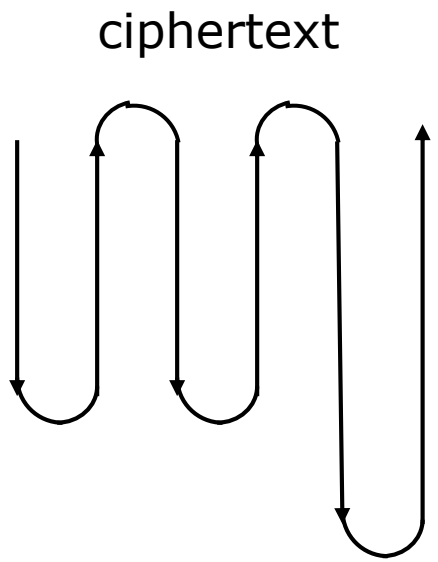


几何图形密码

- 以一种形式写下消息，以另一种形式读取消息
- 明文：I came I saw I conquered

I	C	A	M	E	I
O	C	I	W	A	S
N	Q	U	E	R	E
					D





密文：IONQC CAIUE WMEAR DESI

第三讲 外国古代密码艺术

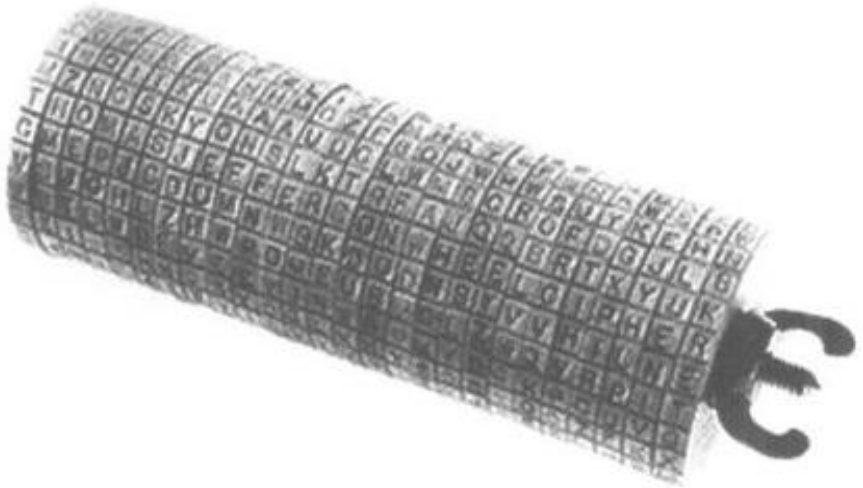
- 代替密码
- 换位密码
- 密码机

杰弗逊密码

- 托马斯·杰弗逊（Thomas Jefferson，1743—1826），美国《独立宣言》的主要作者，并成为第三任美国总统（1801—1809）
- 杰弗逊对密码学深有研究。他在1795年发明了一种密码装置叫做杰弗逊圆盘（Jefferson disk）

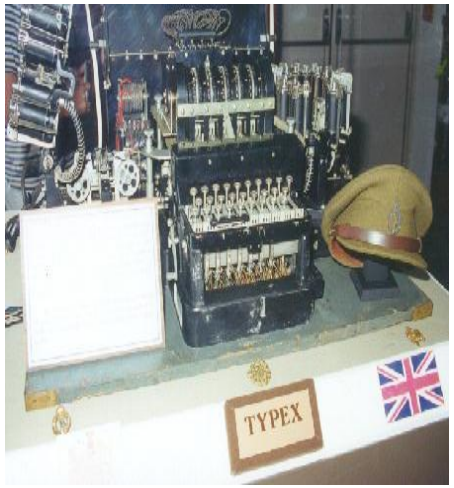
杰弗逊圆盘

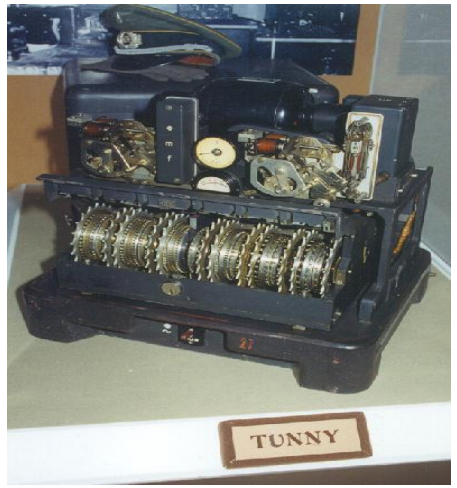
- 这个装置有36片同样大小的木制转轮，套在一根铁杆上。每片转轮的圆周边缘上刻有乱序的26个英文字母
- 转动轮子使明文中的所有字母全排在一条直线上为止．这时圆柱体的其他25行字母也因这一行的固定而被固定了．任选这25行中的一行发出去即为密文.

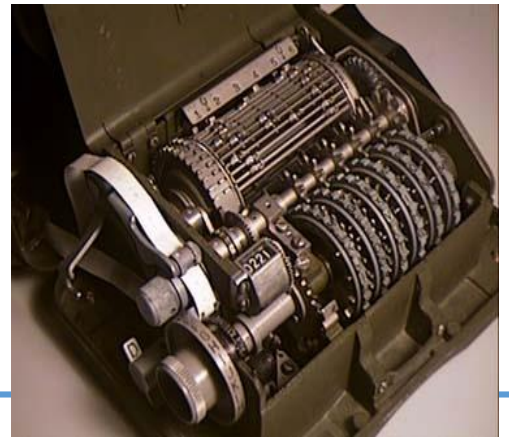


20世纪早期密码机


ENIGMA
© Deutsches Museum


TYPEX


TUNNY



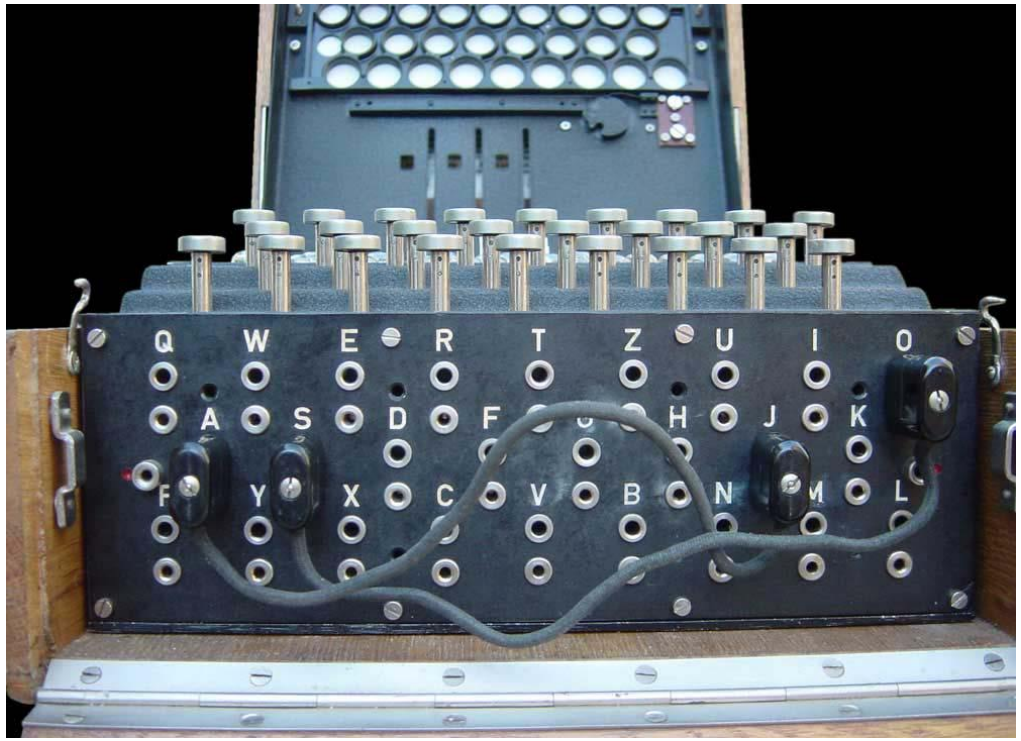

http://hem.passagen.se/tan01/
Hagelin CX-52


KRYHA-CHIFFRIERMASCHINEN
MODELL: COMMERCIAL

Enigma 密码机

- 12kg，28×34×15 cm

德Enigma密码机



Enigma 密码机

- 1918年，德国发明家谢尔比乌斯
  发明了恩尼格玛密码机
  - 密码机30000美金
  - 谢尔比乌斯向企业家们宣称：如果他们重要的商业秘密被竞争对手知道了的话，遭到的损失将比Enigma的价格高得多
- 1923，温斯顿·丘吉尔的著作《世界危机》。
- 从1925年起，谢尔比乌斯的工厂开始系列化生产Enigma，26年德海军开始使用，28年德陆军也开始使用。

破译Enigma

- 以往密码分析员是语言天才，而Enigma是机械装置，波兰总参二局密码处考虑：具有科学头脑的人破译它。
- 1929年1月，波兹南大学给波兰总参二局开列了一张系里最优秀的数学家名单，名单上有后来密码研究的“波兰三杰”。

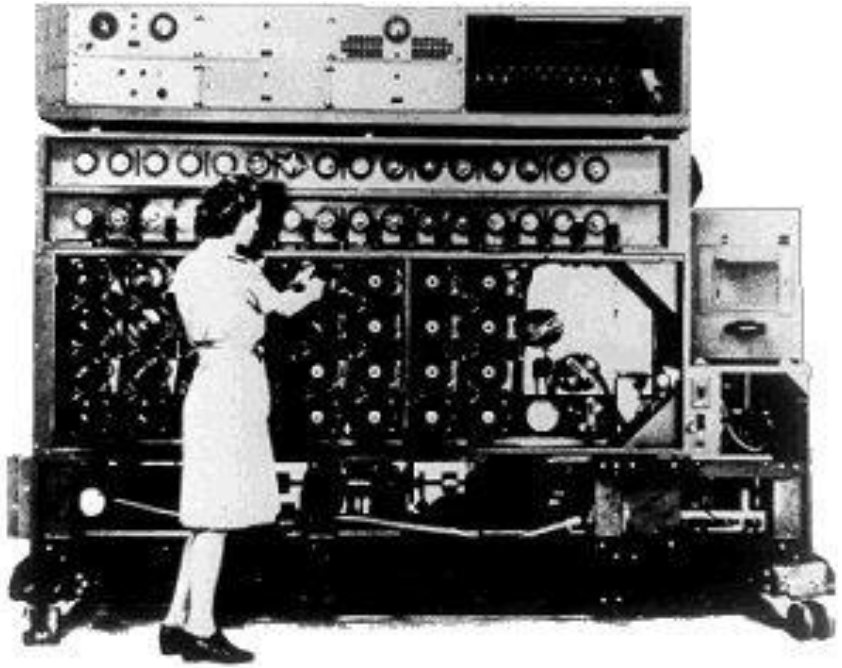
马里安·雷耶夫斯基

杰尔兹·罗佐基

亨里克·佐加尔斯基

破译Enigma

- 波兰三杰设计自动机械计算机 —“密码炸弹”（Bomba ）



破译Enigma

- 在1933年1月到1939年1月这六年，波兰方面一共破译了近十万条德方消息，最重要的有德国在包括苏台德地区兵力重新部署的情报
- 德国人1939年1月加强了密码机的安全性能，但是波兰人的实践表明：
  - Enigma决非坚不可破
  - 数学家在密码分析中的重要作用。
- 英国密码局（40局）以往都是精于文字的语言学家或作家，此后40局开始向牛津、剑桥招聘数学家和数学系学生

感 谢 聆 听!

xynie@uestc.edu.cn