密码：从艺术到科学

刘仁章 2023.09.02

密码学

- 密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。
- 密码编码学（设计）、密码译码学（分析）
- 密码与口令

Atbash Cipher

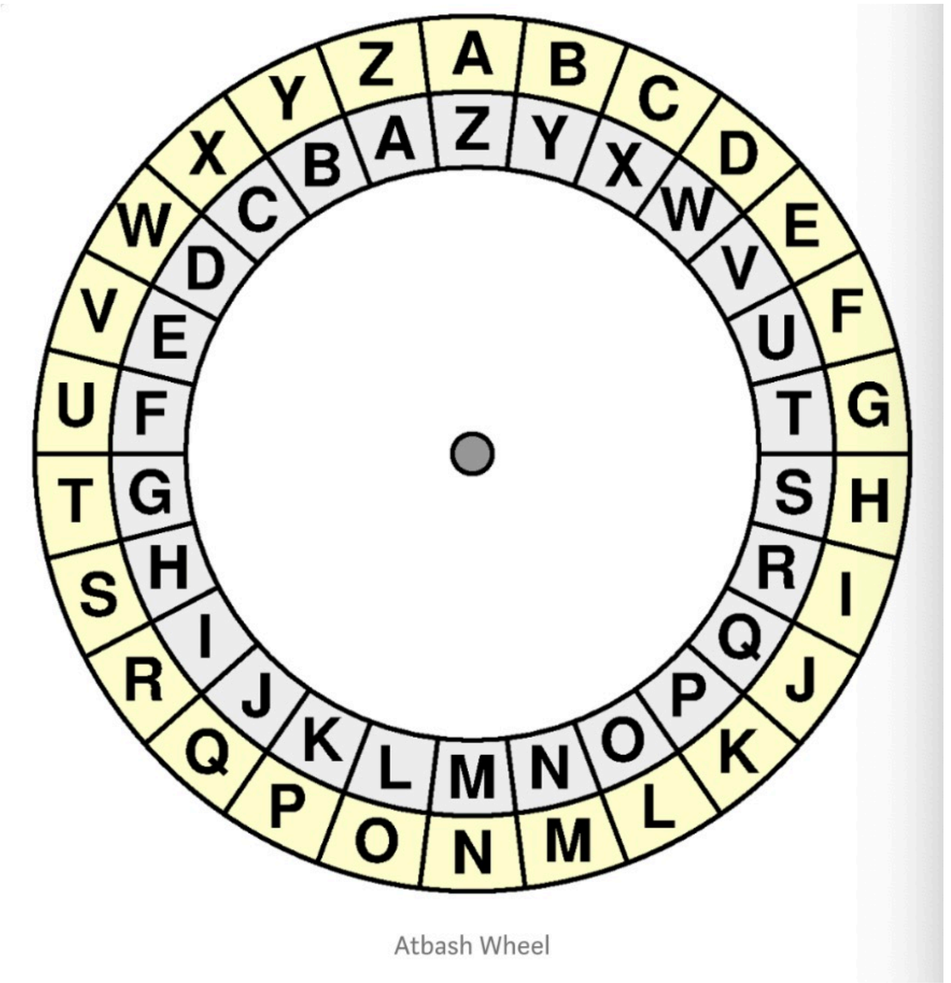
CRYPTOGRAPHY

↓ 加密

xibkgltizksb

↓ 解密

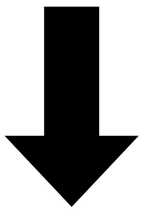
CRYPTOGRAPHY



图片来自于 https://annaspencer.github.io/begincrypto/

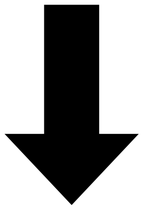
Scytale（密码棒）

scytale is a permutation cipher



加密

serihcimoeysunrtatcapailetp



解密

scytale is a permutation cipher

图片来自于维基百科： https://en.wikipedia.org/wiki/Scytale

几个名词

- 加密：隐藏信息的含义
- 隐写术：隐藏信息的存在
- 编码：信息的表示、可靠传输（摩斯“密”码、汉明码、哈夫曼编码）

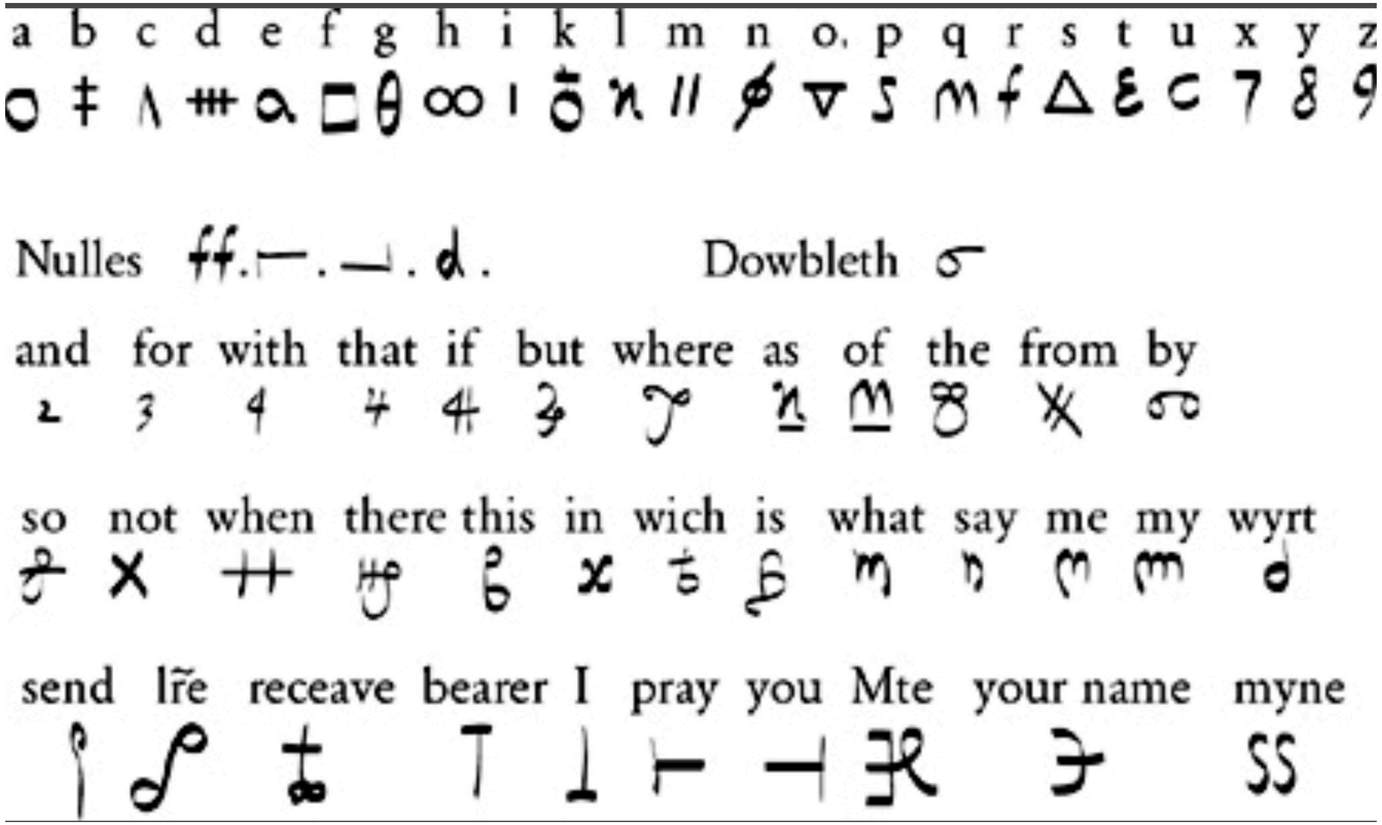
其他一些不常见的密码

- 猪圈密码，当铺密码，培根密码，栅栏密码
- 方言
- ……
- 主要思想：代换（Substitution）和换位（Transposition）置换（Permutation）

巴宾顿阴谋

- 玛丽女王（Mary Queen of Scots）
- 伊丽莎白女王（Queen Elizabeth）
- 沃尔辛厄姆（Sir Francis Walsingham）：情报大臣
- 菲利普斯（Thomas Phelippes）：破译专家
- 巴宾顿（Sir Anthony Babington）
- 吉福德（Gilbert Gifford）：双面间谍，牧师

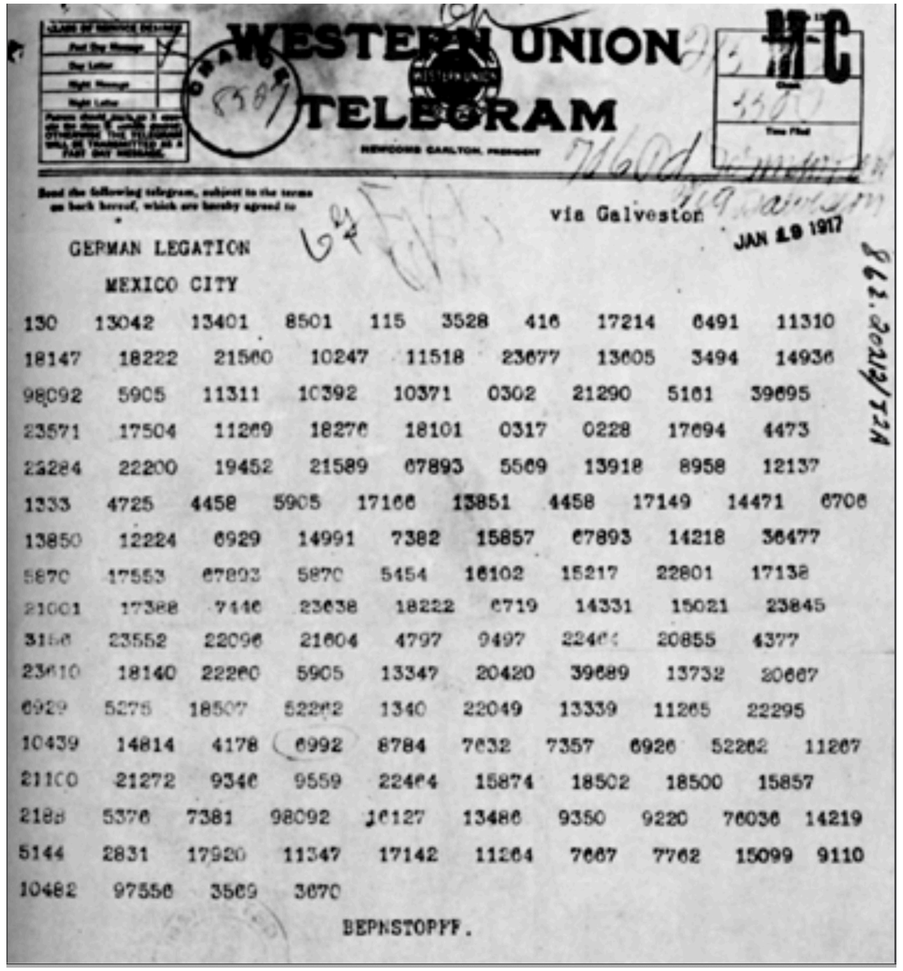
巴宾顿阴谋



图片来自于 The Code Book 一书

齐默尔曼电报事件

- 一战期间的密码破译事件。它使得美国举国震怒，结束中立，最终加入到对德作战的行列中。



WESTERN UNION TELEGRAM

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTOPFF.

图片来自于 The Code Book 一书

破译天才池步洲

- 破译日军偷袭珍珠港的密电。
- 破译日本外务省与海军之间的密电，掌握了山本五十六视察部队的行程。

豪密

- 周恩来设计
- 直到国民党倒台也未被破译出来

近代密码学

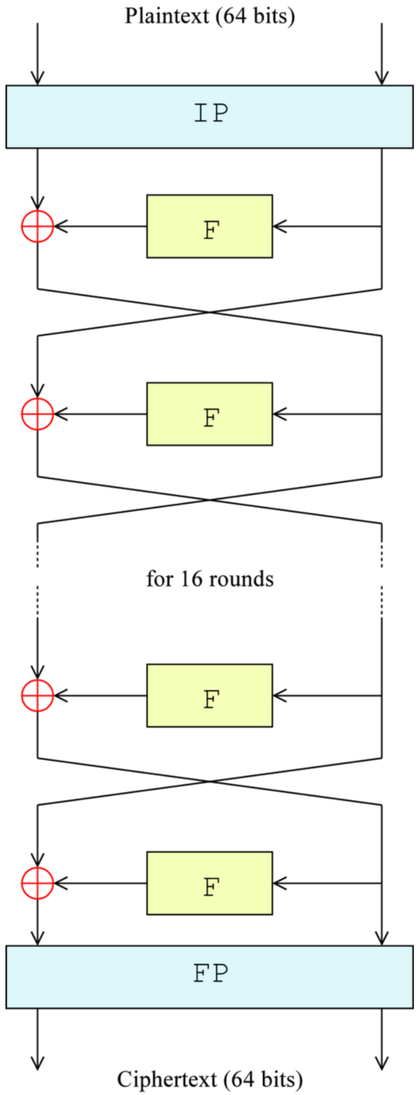
- 香农：保密系统的通信理论（Communication Theory of Secrecy Systems）
- 对称密码设计的原则：扩散（Diffusion）和混淆（Confusion）
- 密码从艺术成为了科学
- 一次一密（One-Time Pad）：完善保密性（Perfect Secrecy，“绝对安全”）
- 流密码

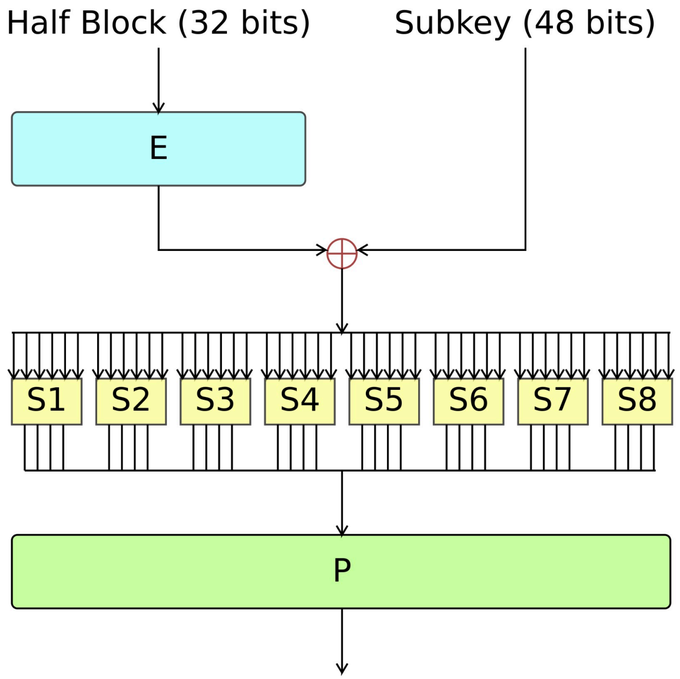
Kerckhoffs原则

- 密码系统仍应是安全的，即使系统（除密钥外）的所有内容都是公开的。即密码系统的安全性仅仅依赖于密钥（而不是算法）的保密性。
- 香农：“敌人知道系统（the enemy knows the system）”。

DES

- 第一个标准化的加密算法
- 从军事、外交领域走向民用





左图为 DES 算法的流程图（Feistel 结构），右图为 DES 算法的 Feistel 结构中的轮函数。图片来自于维基百科：https://en.wikipedia.org/wiki/Data_Encryption_Standard

公钥密码学

- 密钥分配的问题
- Diffie、Hellman：密码学新方向（New Directions in Cryptography）
- Merkle Puzzles
- Rivest，Shamir，Adelman
- James Henry Ellis，Clifford Cocks，Malcolm Williamson

推荐阅读书籍（历史）

- David Kahn: "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet", edition Rev Sub, 1996, Scribner. ISBN 978-0-684-83130-5
- Simon Singh: "The Code Book: The Secret History of Codes and Code-breaking", 2000, New edition, Fourth Estate, ISBN-13: 978-1857028898

量子密码

- 利用量子力学原理，进行密钥分发。
- BB84协议

后量子密码

- Shor 算法
- Grover 算法
- 基于“量子困难”的数学难题构建的密码
- 基于格、多变量、编码、哈希、同源等

密码分类

- 我国密码实行分类管理。密码分为核心密码（核密）、普通密码（普密）和商用密码（商密）。
- 核心密码、普通密码用于保护国家秘密信息。核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级。国家秘密的密级分为绝密、机密、秘密级。商用密码用于保护不属于国家秘密的信息。

商用密码标准

- 我国商用密码标准体系主要包括商用密码国家标准、行业标准。
- 商用密码国家标准由国家标准化管理委员会（全国信息安全标准化技术委员会，信安标委）组织制定，代号为GB，如 GB/T 32918（SM2）。
- GB、GB/T，GB/Z
- 商用密码行业标准由国家密码管理局（国密局）组织制定，报国家标准化管理委员会备案，代号为GM。

商密算法

- SM1/2/3/4/7/9，ZUC
- SM1，SM7算法不公开。
- SM3是密码哈希函数。
- SM4，ZUC是对称加密算法。
- SM2，SM9是公钥密码算法。

密评

- 商用密码应用安全性评估。GB/T 39786
- 关键信息基础设施、政务信息系统、等保三级以上信息系统建设，都要“过密评”。
- 密评机构

中国密码学会

- 中国密码学会
- 《密码学报》

密码比赛

- 全国密码科普竞赛
- 全国密码技术竞赛
- 全国高校密码数学挑战赛
- “熵密杯”密码应用安全竞赛
- “金融密码杯”全国密码应用和技术创新大赛
- NSUCRYPTO： https://nsucrypto.nsu.ru/ 每年一次，9，10月
- IACR CHES每年举办一次 Challenge
- Crypto CTF（欢迎提供相关信息）

课程与培训

- 密码学会高端培训：中国密码学会，每年暑假举办
- BIU Winter School on Cryptography
- Dan Boneh 公开课
- TheIACR Courses：https://www.classcentral.com/institution/iacr

网站

- http://www.practicalcryptography.com/
- Simon Singh 主页： https://simonsingh.net/cryptography/
- Bruce Schneier 主页： https://www.schneier.com
- Project Euler. https://projecteuler.net 数学编程解题网站

工具

- CrypTool： https://www.cryptool.org/en/
-

课后题网站

- https://github.com/primihub/crypto-learning