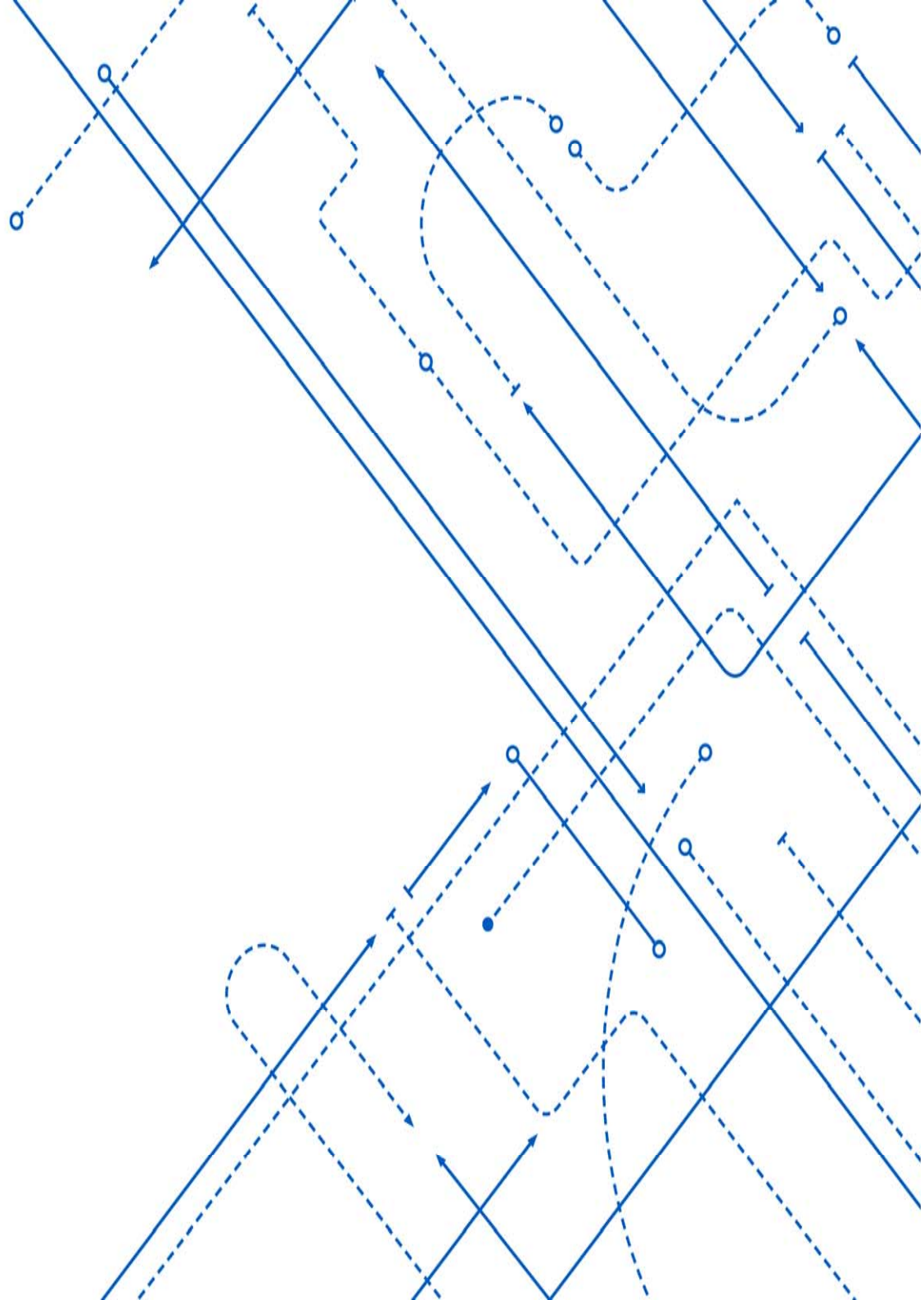
密码学

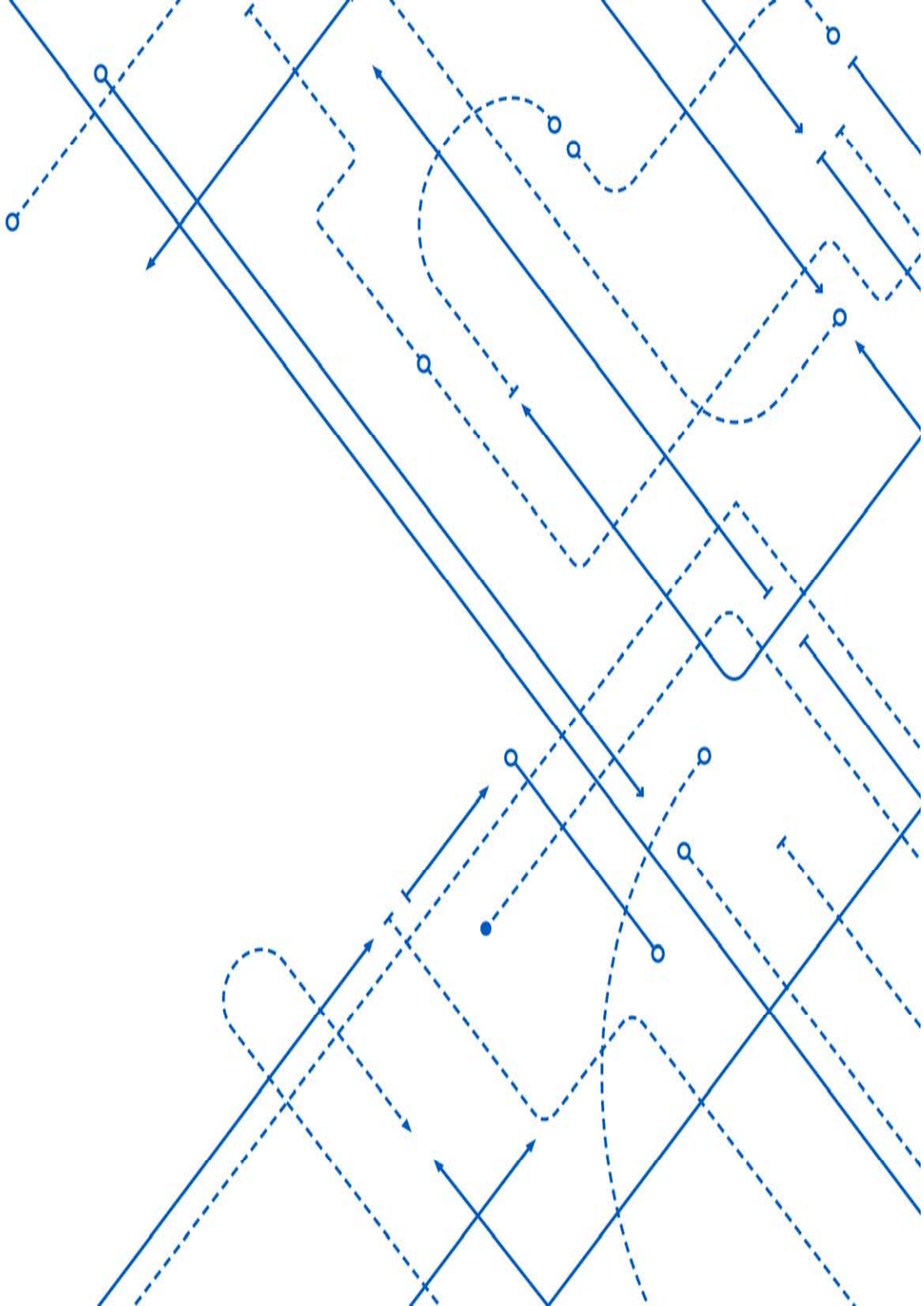
教师：张帆 fanzhang@zju.edu.cn

助教：陈欢 chen_huan@zju.edu.cn

浙江大学 ZHEJIANG UNIVERSITY



课程介绍



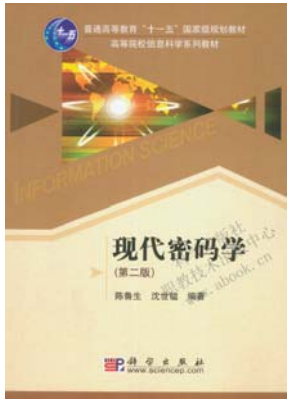
浙江大学
ZHEJIANG UNIVERSITY

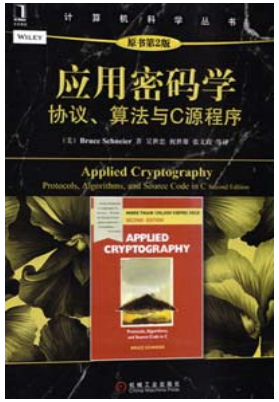
内容安排

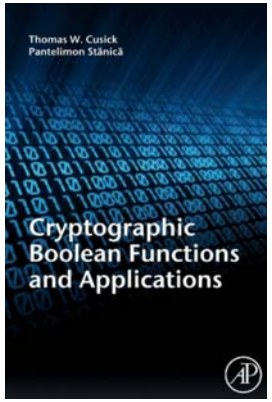
- 数学基础
- 古典密码
- Hash函数
- 分组密码工作模式与流密码
- DES算法和AES算法
- RSA算法
- 椭圆曲线算法

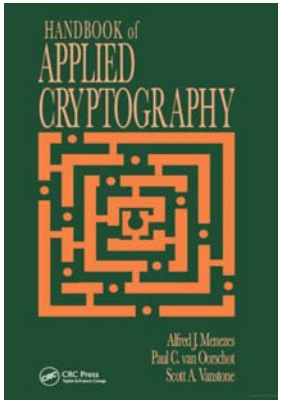
参考书目

- 中文：现代密码学（第二版），陈鲁生、沈世镒. 科学出版社，2008. ISBN: 9787030226617 。
- 中文：应用密码学:协议算法与C源程序，Bruce Schneier (作者)，吴世忠
- 英文影印版：Cryptographic Boolean Functions and Applications, Thomas W. Cusick , Pantelimon Stanica
- Handbook of Applied Cryptography (应用密码学手册)









参考网站

- 白洪欢老师的个人教学网站
- http://10.71.45.100/bhh

进度

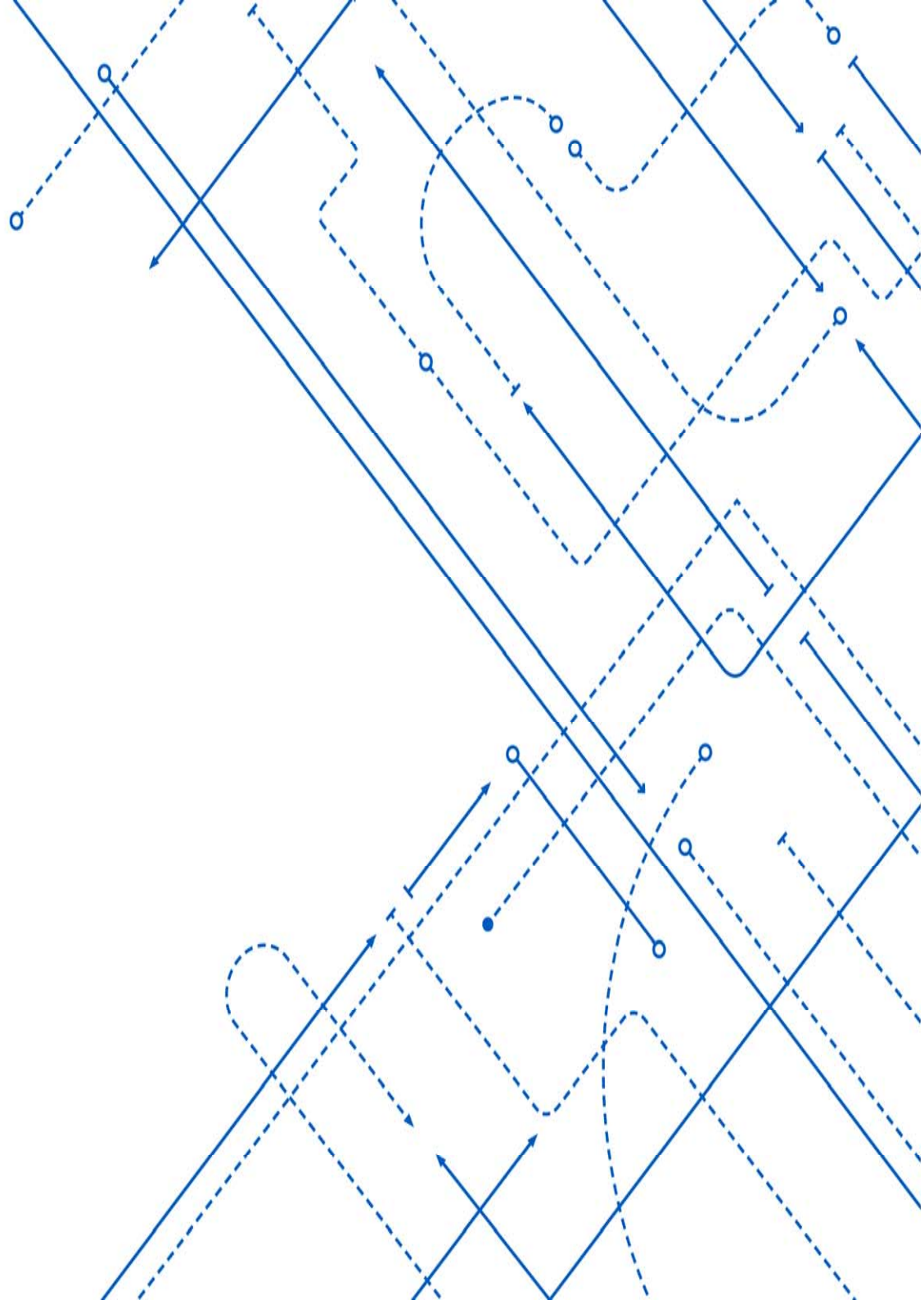
- 第一章（简介）： 2
- 第二章（古典密码）： 6
- 第三章（哈希函数）： 4
- 第四章（加密模式和流密码）： 4
- 第五章（对称DES和AES）： 6
- 第六章（非对称RSA）： 4
- 第七章（椭圆曲线）： 4
- 复习: 2

考核安排

- 期末考试（60%）

- 平时成绩（40%）
  - 四次编程作业
  - PTA平台

第1章 数学基础

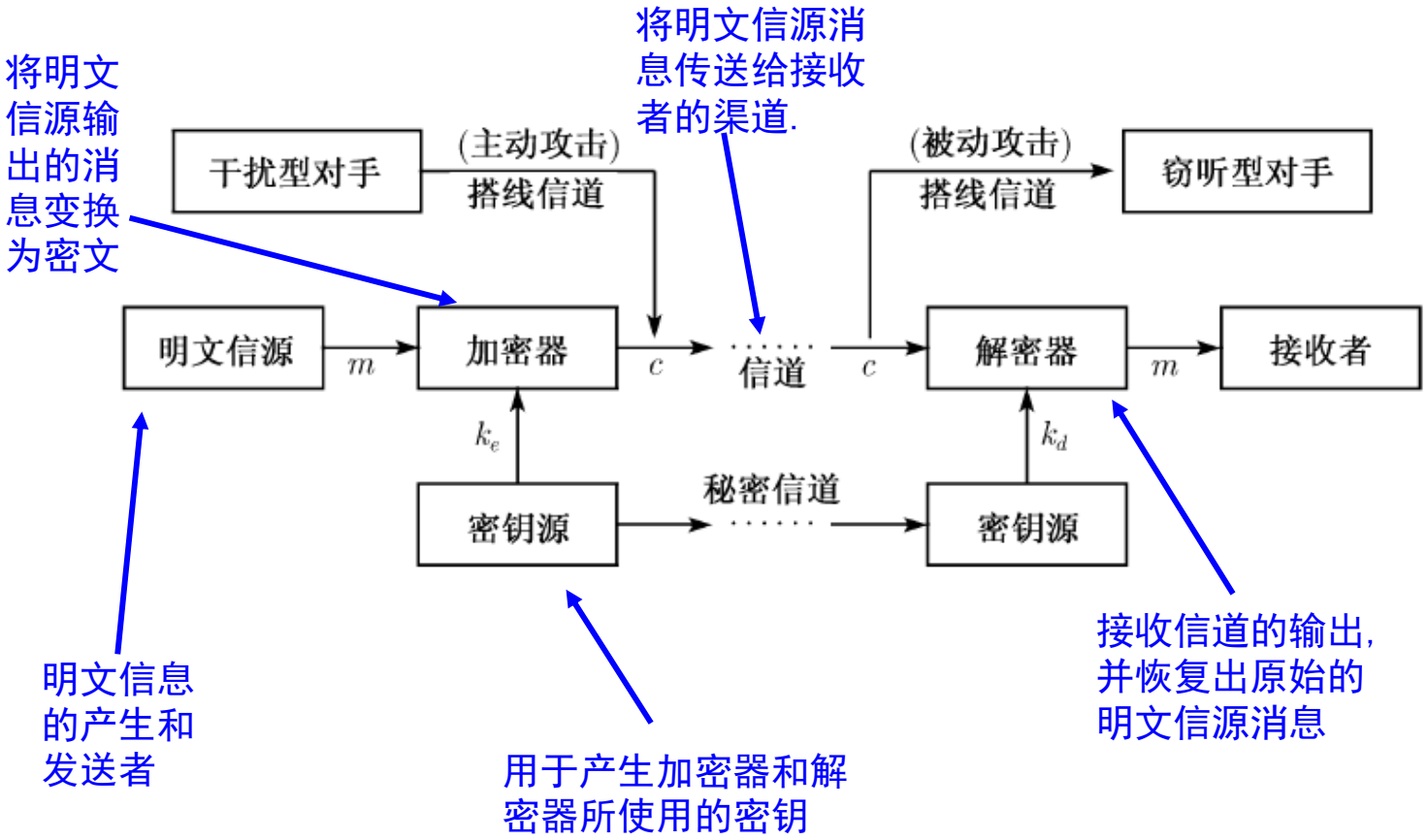


浙江大学
ZHEJIANG UNIVERSITY

目录

CONTENTS

保密系统


将明文信源输出的消息变换为密文
将明文信源消息传送给接收者的渠道.
干扰型对手
(主动攻击)
搭线信道
(被动攻击)
搭线信道
窃听型对手
明文信源
m
加密器
c
信道
c
解密器
m
接收者
k_e
k_d
秘密信道
密钥源
密钥源
明文信息的产生和发送者
用于产生加密器和解密器所使用的密钥
接收信道的输出,并恢复出原始的明文信源消息

关键事件

- 1967年： David Kahn 出版了 “The Codebreakers”

أصول علم التعمية واستخراج المعمى عند العرب

Arabic Origins of Cryptology

د. محمد بن إبراهيم السويل

مدينة الملك عبد العزيز للعلوم والتقنية

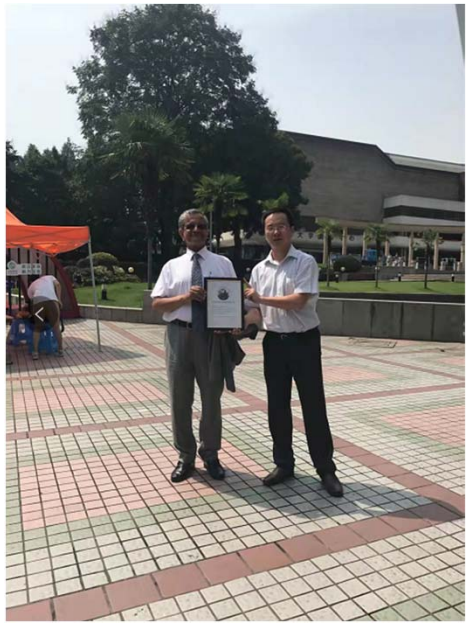
Mohammed I. Al-Suwaiyel, PhD

King Abdul Aziz City for Science and Technology, KACST

默罕默德 苏韦仪 博士

沙特阿拉伯王国

阿卜杜勒-阿齐兹国王科技城

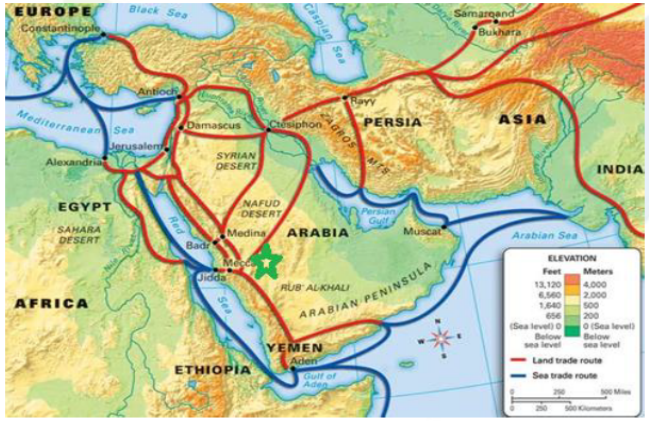


关键事件

➢ 1967年： David Kahn 出版了 “ The Codebreakers ”

The Discovery of 15 Ancient Arabic Manuscripts on Cryptology

❖ In 1967 David Kahn, a prominent historian of cryptology, referred to al-Qalqashandi's book, and the reference to ibn ad-Durayhim's work on methods to "conceal secrets.



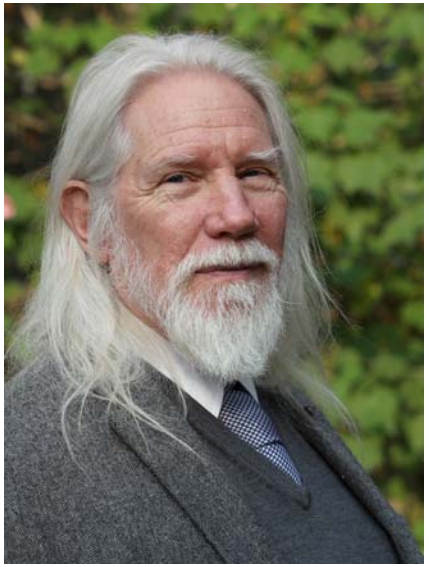
➢ **Major trade routes crossing the Arabian Peninsula around 570BC. *Note the overlap with the Silk Road***

❖ Kahn wrote: ***"Cryptology was born among the Arabs. They were the first to discover and write down the methods of cryptanalysis. The people that exploded out of Arabia in the 600s AD and flamed over vast areas of the known world swiftly engendered one of the highest civilizations that history had yet seen."***

➢ **The Codebreakers , The Story of Secret Writing, David Kahn, 1967, The Macmillan Company**

关键事件

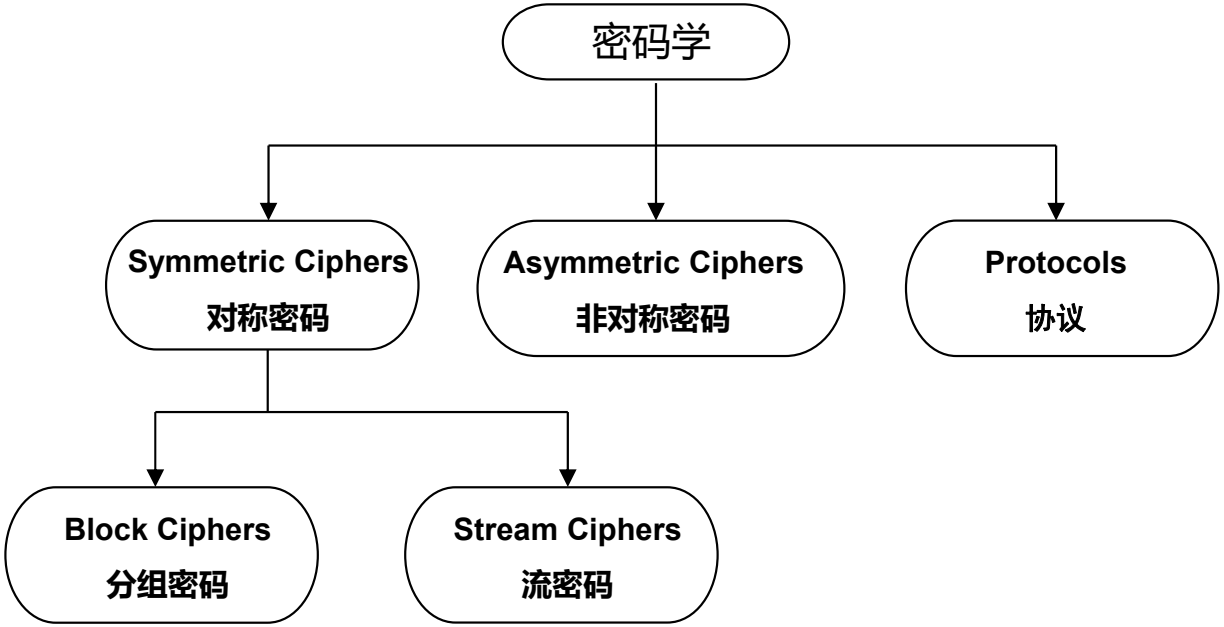
- 1967年： David Kahn 出版了 “The Codebreakers”
- 1970年：IBM采用“Lucifer”密码系统
- 1975年：公钥密码学的提出和发展



关键事件

- 1967年： David Kahn 出版了 “The Codebreakers”
- 1970年：IBM采用“Lucifer”密码系统
- 1975年：公钥密码学的提出和发展
- 1981年：第一届国际密码讨论年会CRYPTO （Annual International Cryptology Conference）
  - Crypto、EuroCrypt、AsiaCrypt、CHES
  - RealWorld Crypto

密码学领域分类


密码学
Symmetric Ciphers
对称密码
Asymmetric Ciphers
非对称密码
Protocols
协议
Block Ciphers
分组密码
Stream Ciphers
流密码

对称/非对称密码体制

- 对称密码体制(symmetric cryptosystem)：
  - 加密及解密使用同一密钥。
  - 或者一个密钥很容易从另一个密钥计算得到。
  - 从古代到1976年的所有加密方案都是对称的。
  - 例如，用于加密和消息身份验证。
- 非对称密码体制(asymmetric cryptosystem)：
  - 公钥系统
  - 使用不同的密钥进行加密和解密。
  - 加密密钥简称公钥(public key)，解密密钥简称私钥(private key)。
  - 计算上不可能从一个密钥推导出另一个密钥。
  - 1976年，Diffie、Hellman和Merkle公开提出了公钥（或非对称）密码。
  - 例如，用于密钥交换和数字签名。

常见密码

- 对称密码：
  - 古典密码
  - 分组密码
    - 分组密码工作模式
      - 电子密码簿ECB
      - 密文块链接模式CBC
      - 密文反馈模式CFB
      - 输出反馈模式（OFB）
      - 计数器模式（CTR）
    - 数据加密标准：DES算法
    - 高级加密标准：AES算法
  - 流密码
    - RC4

常见密码

- 非对称密码：
  - RSA
  - 椭圆曲线(Elliptic Curve)算法
  - DH
  - ElGamal
  - DSA
  - ECDSA

常见密码原语

- 报文摘要（Message digests）：
  - plaintext 明文 ←→ ciphertext 密文 一般密码，双向加密/解密
  - message → digest 报文转化为摘要, 相当于有损压缩，单向加密，中间不需要密钥
  - 举例：
    - MD5
    - SHA

轻量级（分组）密码

- 理想特性：
- 分组密码的目的是提供密钥伪随机置换，然后将其用作更复杂协议的构造块。“好的”分组密码必须快速且安全，即具有实际计算能力的对手即使可以访问能够加/解密选择的明文的黑盒也不可能检索到使用的密钥（针对选择的密文攻击的安全性）。
- 设计原则：
- 分组密码有两类设计：SP网络（Substitution-Permutation Network）和Feistel网络。在设计轻量级分组密码时，也有特定的限制。首先，内存非常昂贵，因此实现S盒作为查找表可能会占用大量硬件空间。这就是为什么这些密码通常根本没有S盒（SIMON）或非常小的S盒，只有4x4（PRESENT）。

轻量级（分组）密码

- Feistel网络
  - 一种迭代密码，其中的内部函数称为轮函数。加密和解密操作非常相似，在某些情况下甚至是相同的，只需要逆转密钥编排。因此，实现这种密码所需的代码或电路大小能几乎减半。
- SP网络
  - 旨在使用两种不同的操作提供混淆和扩散。“混淆”的目的是使明文、密钥和密文之间的关系变得复杂，而“扩散”的目的是实现雪崩效应，即对明文的一个小修改必须扩展到整个密文。
  - 在SPN中，混淆由一层S盒执行。S盒只是明文空间的一小个子集的排列，许多S盒并行使用以作用于整个明文。扩散是通过使用整个空间的排列来实现的，通常是线性的，有时也称为P盒。

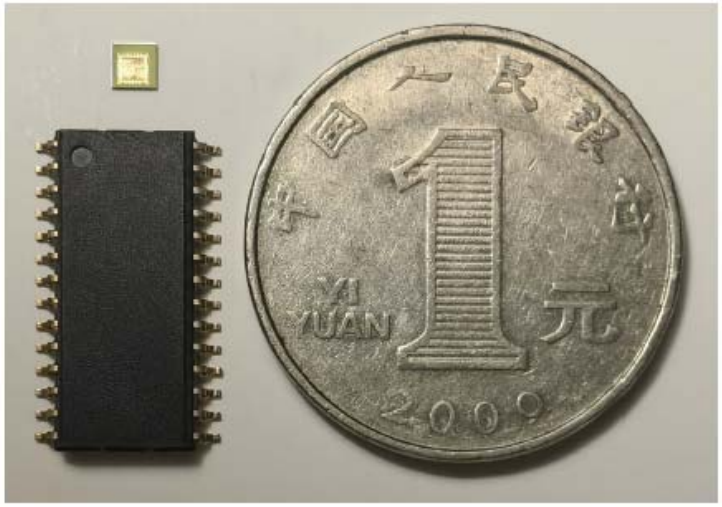
认证加密算法

- 认证加密（Authenticated encryption，AE）和带有关联数据的认证加密（authenticated encryption with associated data，AEAD，AE的变种）是一种能够同时保证数据的保密性、 完整性和真实性的一种加密模式。这些属性都是在一个易于使用的编程接口下提供的。
- 人们观察发现安全地将保密模式与认证模式组合可能是容易出错和困难的，于是认证加密应运而生。这一点已由许多实际攻击证实，这些攻击通过对身份验证（包括SSL与TLS）的不正确实现或缺失，引入到了生产协议和应用程序中。

认证加密算法- CAESAR竞赛

- CAESAR（Competition for Authenticated Encryption: Security, Applicability, and Robustness）竞赛是由NIST和Dan Bernstein共同发起的密码算法竞赛，旨在征集综合性能和安全性优于AES-GCM的认证加密算法，能够同时实现数据的机密性和完整性保护。最后入围的算法可能被推荐至工业界并标准化。
- CAESAR竞赛从2013年1月开始，整个竞赛活动持续6年时间，于2019年2月宣布7个算法获选最终算法集。CAESAR竞赛旨在增强人们对认证加密算法的认识和信心。

认证加密算法- Ascon



(a) Optical photo of die and packaged chip

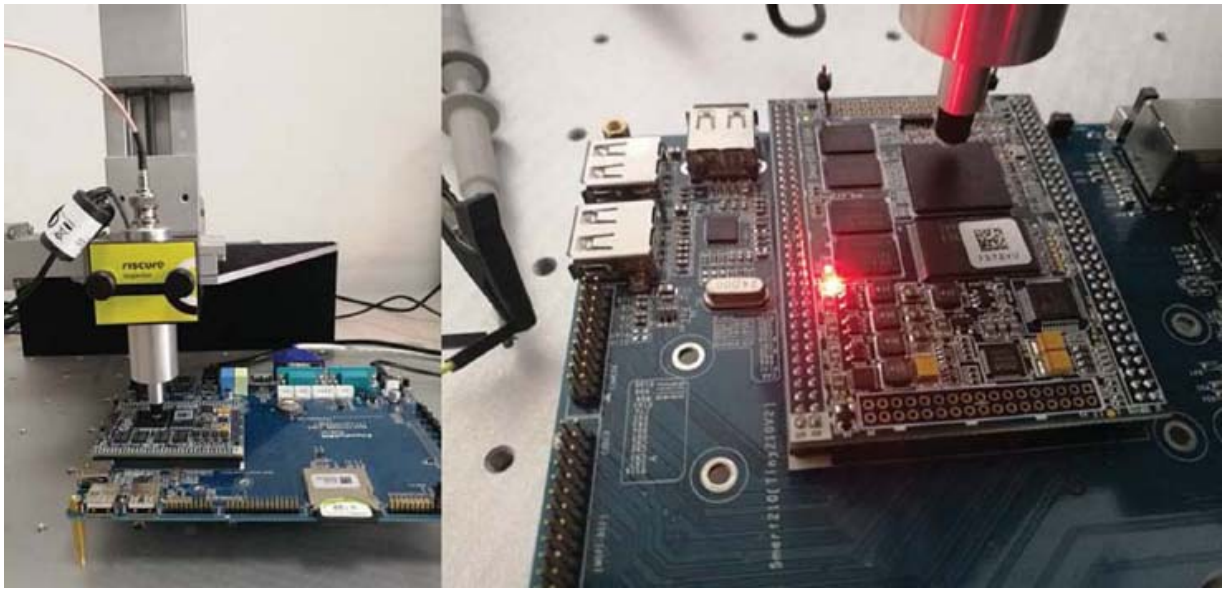
后量子密码

- 后量子密码学（Post-quantum cryptography，PQC），又称抗量子计算密码学，是密码学的一个研究领域，专门研究能够抵抗量子计算机的加密算法，特别是公钥加密（非对称加密）算法。
- 新的密码漏洞的发现和密码分析技术的突破往往会导致之前的密码算法被淘汰。量子计算技术的出现将危及当前许多密码算法，尤其是广泛用于保护数字信息的公钥密码算法。
- 不同于量子密码学，后量子密码学使用现有的电子计算机，不依靠量子力学，它依靠的是密码学家认为无法被量子计算机有效解决的计算难题。

后量子密码

- 在公钥加密方面，后量子密码学的研究方向包括：
  - 格密码学（Lattice-based cryptography）
    - 在算法构造本身或其安全性证明中应用到格的密码学。
  - 多变量密码学（Multivariate cryptography）
    - 应用了有限域F上多元多项式的密码学，包括对称加密和非对称加密。
  - 散列密码学（Hash-based Cryptography）
    - 应用散列函数的数字签名。
  - 编码密码学（Code-based Cryptography）
    - 应用了编码理论与纠错码的密码学。
  - 超奇异椭圆曲线同源密码学（Supersingular elliptic curve isogeny cryptography）
    - 利用超奇异椭圆曲线与超奇异同源图的数学性质的密码学，可以实现超奇异同源密钥交换（SIDH），具有前向安全性。
  - 容错学习问题（LWE）

后量子密码-SIKE



目录

CONTENTS

整除

- 整除的定义:
  - 设a、b均为整数,且a≠0, 若存在整数k使得b=a*k，则称a整除b，记作a|b。（b是a的整数倍）

- 整除相关的3个命题:
  - ①对于任意整数a，都有1|a；若a≠0，则有a|0且a|a。
  - ②若a|b且b|c，则a|c。
  - ③若a|b且a|c，则a|(s*b+t*c)，其中s、t为任意整数。

素数与互素

- 素数的定义:
  - 若整数p只有因子±1及±p, 则称p为素数。
- 互素(relatively prime)的定义:
  - 对于整数a、b，若gcd(a,b)=1，则称a、b互素。
  - a=3, b=5 gcd(a,b)=1
  - a=3, b=4 gcd(a,b)=1
  - a=4, b=9 gcd(a,b)=1
- 素数相关的定理:
  - 任一整数a(a>0)都能唯一分解成以下形式:
  - $a = p_1 * p_2 * p_3 * \ldots * p_t$
  - 其中p_1、p_2、p_3、…、p_t是素数。

最大公约数(greatest common divisor)

- 定义：
  - 指能够整除多个整数的最大正整数，而多个整数不能都为零。
  - 例如8和12的最大公约数为4，gcd(8,12) = 4。
  - 如果两数的最大公约数为1，那么这两个数互素。

- gcd相关的定理（裴蜀定理）：
  - 设a、b为整数，且a、b中至少有一个不等于0，令d=gcd(a,b)，则一定存在整数x、y使得下式成立: a*x + b*y = d

- 特别地，当a、b互素时，则一定存在整数x、y使得 a*x+b*y=1 成立。

欧几里德算法（Euclidean algorithm）

- 又称辗转相除法，能有效找出两数的最大公约数。
- 原理：两个整数的最大公约数等于其中较小的数和两数相除余数的最大公约数。
- 利用欧几里德算法计算gcd(a,b)：
  - EUCLID(a,b)
  - 1. A = a; B = b
  - 2. if B = 0 return A = gcd(a, b)
  - 3. R = A mod B
  - 4. A = B
  - 5. B = R
  - 6. goto 2

欧几里德算法-举例

- 计算gcd(1970,1066)：
  - 1970 = 1 x 1066 + 904　　gcd(1066, 904)
  - 1066 = 1 x 904 + 162　　gcd(904, 162)
  - 904 = 5 x 162 + 94　　gcd(162, 94)
  - 162 = 1 x 94 + 68　　gcd(94, 68)
  - 94 = 1 x 68 + 26　　gcd(68, 26)
  - 68 = 2 x 26 + 16　　gcd(26, 16)
  - 26 = 1 x 16 + 10　　gcd(16, 10)
  - 16 = 1 x 10 + 6　　gcd(10, 6)
  - 10 = 1 x 6 + 4　　gcd(6, 4)
  - 6 = 1 x 4 + 2　　gcd(4, 2)
  - 4 = 2 x 2 + 0　　gcd(2, 0)

由于最终得到mod b=0（即无余数），终止运算。
答案是最后一个非零值。
在这种情况下，gcd（1970，1066）=2。

同余(congruent)的定义

- 设a、b、n均为整数，且n≠0，当a-b是n的倍数时即a=b+n*k(k为整数)，我们称a、b对于模n同余(a is congruent to b mod n)，记作：$a \equiv b \pmod{n}$
- 可以理解为：a%n == b %n
  - 例如：$1 \equiv 4 \bmod 3$
  - 例如：$5 \equiv 8 \bmod 3$

- 模运算在密码学中的优势：
  - 保证明文和密文在某个区间内，例如，一个字节的大小。
  - 增加破译密钥的难度。

同余相关的命题

- 设a,b,c,d,n均为整数，且n≠0，则有
- ①当且仅当n|a时，有a≡0 (mod n)　　即 n是a的整数倍
- ②a≡a (mod n)
- ③当且仅当 b≡a (mod n)时, 有a≡b (mod n)
- ④若a≡b 且 b≡c (mod n)，则一定有：
  - a≡c (mod n)
  - a = k*n+x
  - b = k'*n+x
  - c = k''*n+x
- ⑤若a≡b (mod n)且c≡d (mod n)，则有：
  - a+c≡b+d, a-c≡b-d, a*c≡b*d (mod n)

加法模逆元

- 定义: 若a+b≡0 (mod n), 则称a是b的加法模n逆元，b是a的加法模n逆元。
- 例如：恺撒加密法在解密时会用到加法逆元
  - 恺撒加密法：替换加密，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。
  - 通过排列明文和密文字母表，密文字母表示通过将明文字母表向左或向右移动一个固定数目的位置。例如，当偏移量是左移3的时候（解密时的密钥就是3）：

    明文字母表： ABCDEFGHIJKLMNOPQRSTUVWXYZ

    密文字母表： DEFGHIJKLMNOPQRSTUVWXYZABC

加法模逆元-举例

明文字母表： ABCDEFGHIJKLMNOPQRSTUVWXYZ

密文字母表： DEFGHIJKLMNOPQRSTUVWXYZABC

- 加密过程: y = (x+3) % 26
- 解密过程: x = (y+23) % 26
- 因为23是3的加法逆元, 即23相当于-3
- -3 = -26+23 = 23 mod 26

- 加密算法: y=(x-'a'+3)%26 + 'a';
- 解密算法: x=(y-'a'+23)%26 + 'a';
- 3+23 ≡ 0 (mod 26) 表示3的加法逆元是23
- 3-3 ≡ 0 (mod 26) 表示3的加法逆元是-3
- 所以 -3 ≡ 23 (mod 26)
- 或者这样推理: -3 % 26 == (-26+23) % 26 == 23 % 26

乘法模逆元

- 定义: 若a*b≡1 (mod n), 则称a是b的乘法模n逆元，b是a的乘法模n逆元。
- a的乘法逆元记作a^{-1}。

- 常用于加密算法中，如仿射算法。

- 举例： 求13模35的乘法逆元
  - 设13模35的乘法逆元为x，则 13*x ≡ 1 (mod 35)
  - 上述等式成立的充要条件为 gcd(13,35)=1 即互素
  - 于是一定存在x、y使得13*x + 35*y = 1成立，利用扩展欧几里德法(extended Euclidean algorithm)（辗转相除法）可以解出上述方程中的x及y，其中的x就是13模35的逆元。

乘法模逆元-举例

- 举例：求13模35的乘法逆元
  - 设13模35的乘法逆元为x，则 13*x ≡ 1 (mod 35)
  - 上述等式成立的充要条件为 gcd(13,35)=1 即互素
  - 于是一定存在x、y使得13*x + 35*y = 1成立，利用扩展欧几里德法(extended Euclidean algorithm)（辗转相除法）可以解出上述方程中的x及y，其中的x就是13模35的逆元。

逐层替换，合并同类项

35=2*13+9
13=1*9+4
9=2*4+1

1 = 9-2*4
= 35-2*13 – (13-1*9)*2
= 35-2*13 – (13-(35-2*13))*2
= (35-2*13)*3 – 13*2
= 35*3 – 8*13

x=-8, y=3
-8 ≡ (-35+27) ≡ 27 (mod 35)
13 * (-8) = 1 mod 35
13 * (-35*27) = 13*(-35) + 13*27
= 13*27
= 1 mod 35

所以13模35的乘法逆元为27。

扩展欧几里德法

- EXTENDED EUCLID(m, b)
- 1. (A1, A2, A3)=(1, 0, m);
- (B1, B2, B3)=(0, 1, b)
- 2. if B3 = 0
- return A3 = gcd(m, b); no inverse
- 3. if B3 = 1
- return B3 = gcd(m, b); $B2 = b^{-1} \bmod m$
- 4. Q = A3 div B3
- 5. (T1, T2, T3)=(A1 − Q B1, A2 − Q B2, A3 − Q B3)
- 6. (A1, A2, A3)=(B1, B2, B3)
- 7. (B1, B2, B3)=(T1, T2, T3)
- 8. goto 2

扩展欧几里德法-举例

- 举例： 求13模35的乘法逆元

Q	A1	A2	A3	B1	B2	B3
—	1	0	35	0	1	13
2	0	1	13	1	–2	9
1	1	–2	9	–1	3	4
2	–1	3	4	3	-8	1

由于最终得到B3=1，终止运算。
答案是最后的B2。
所以13模35的乘法逆元为-8，即27。

乘法模逆元-举例

- 2的mod 5乘法逆元=3
- 1的mod 5乘法逆元=1
- 3的mod 5乘法逆元=2
- 4的mod 5乘法逆元=4
- 2的mod 6乘法逆元=不存在，因为gcd(2,6)=2≠1

Thank you!