现代密码学 样卷

题目中数值均为随机产生 http://bbs.sjtu.edu.cn/bbscon?board=IS&file=M.1225633522.A

Ⅰ安全威胁与防护措施

1.对安全的攻击，从信息流的角度可以分为中断、截获、篡改、伪造。
2.篡改攻击是一种主动攻击。

Ⅱ古典加密

1.用恺撒密码加密 the quick brown fox jumps over the lazy dog，密钥为 6。
znk waoiq hxuct lud pasvy ubkx znk rgfe jum
2.恺撒密码可以扩充为单字母随机替换，用于 26 个英文字母时密钥空间是多大？
密钥空间是 26!。
a 可以选择 26 个字母的任何一个，b 在剩下 25 个字母中选择……
3.为什么恺撒密码不安全？
密钥空间太小。
密文显示了明文的统计规律；例如已知明文为英语，密文足够长时，出现最多的密文字母一定是 e。
4.用 Hill 密码加密 yoursunny，密钥为 $K=\begin{pmatrix}17&17&5\\21&18&21\\2&2&19\end{pmatrix}$
sgotjiqxo
5.用 Hill 密码解密 idzugi，密钥为 $K=\begin{pmatrix}17&17&5\\21&18&21\\2&2&19\end{pmatrix}$
首先求出逆矩阵 $K^{-1}=\begin{pmatrix}4&9&15\\15&17&6\\24&0&17\end{pmatrix}$（从 $\begin{pmatrix}17&17&5&1&0&0\\21&18&21&0&1&0\\2&2&19&0&0&1\end{pmatrix}$ 起，作初等变换成 $\begin{pmatrix}1&0&0&4&9&15\\0&1&0&15&17&6\\0&0&1&24&0&17\end{pmatrix}$）
然后解密得 sjtuis
6.分组长度为 3 的 Hill 密码，已知明文 bbssjtucn 对应的密文是 ofwfmbwbb，破解密钥？
bbssjtucn=[1,1,18,18,9,19,20,2,13]
ofwfmbwbb=[14,5,22,5,12,1,22,1,1]

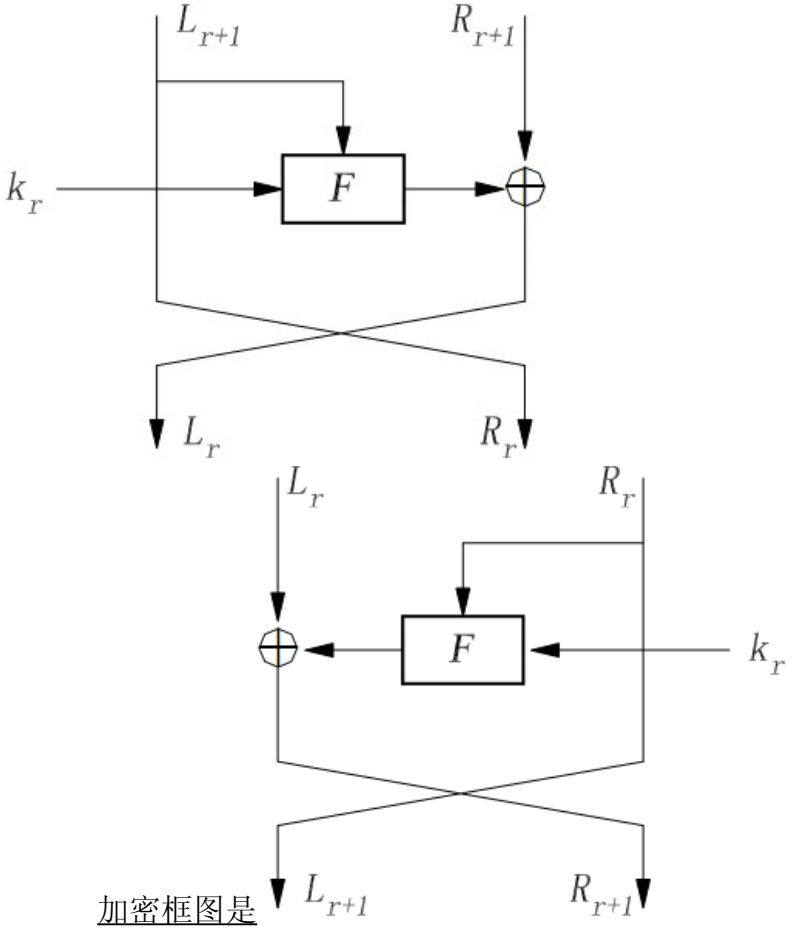
列出线性方程组 $\begin{aligned} 14&=1k_{11}+1k_{12}+18k_{13}\\ 5&=1k_{21}+1k_{22}+18k_{23}\\ 22&=1k_{31}+1k_{32}+18k_{33}\\ 5&=18k_{11}+9k_{12}+19k_{13}\\ 12&=18k_{21}+9k_{22}+19k_{23}\\ 1&=18k_{31}+9k_{32}+19k_{33}\\ 22&=20k_{11}+2k_{12}+13k_{13}\\ 1&=20k_{21}+2k_{22}+13k_{23}\\ 1&=20k_{31}+2k_{32}+13k_{33}\end{aligned}$ ，解得 $K=\begin{pmatrix}1&1&18\\18&9&19\\20&2&13\end{pmatrix}$

Ⅲ分组加密

1.解密密钥可以从加密密钥直接推出的密码算法是对称密码算法。

2. Fiestel 结构有扩散和扰乱的作用，为统计分析制造障碍

3.根据如图的 Fiestel 结构解密框图，画出加密框图



加密框图是

4.求 P 盒[1 7 5 2 4 3 6 9 10 8]的逆

[1 4 6 5 3 7 2 10 8 9]

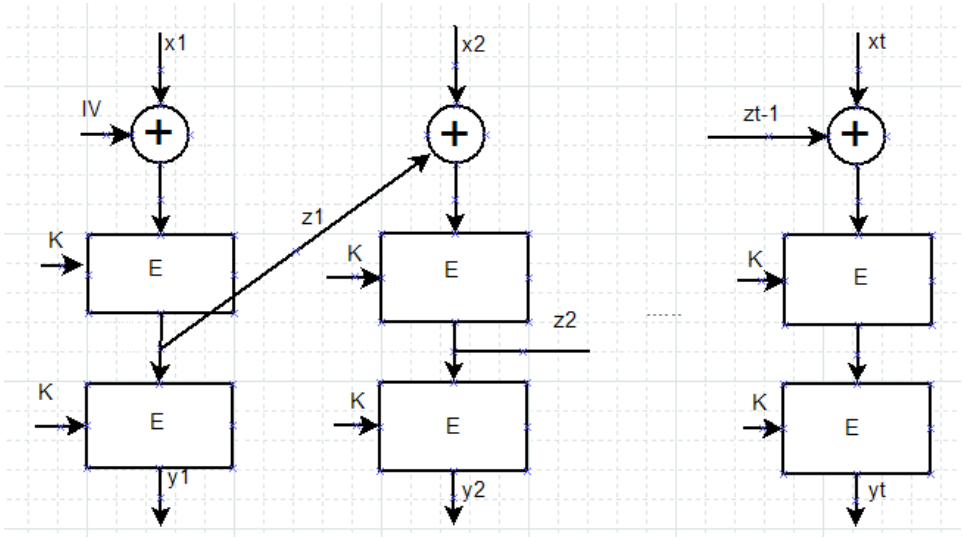
5.用 S-DES 加密……，密钥为……，根据框图加密

略

Ⅳ对称加密算法

1. DES 算法的分组长度 64bit，密钥长度 56bit，分为 16 轮；IDEA 算法的分组长度 64bit，密钥长度 128bit，分为 8 轮

2.如图的工作模式加密框图，画出对应的解密框图



答案略

3. IDEA⊙运算的快速运算表示为 $a \odot b = \begin{cases} C_L - C_H + C_0 \\ C_L - C_H + (2^{16}+1) \end{cases}$ ，其中的 C_L、C_H、C_0 是什么？

2. Binary Modulo 2^n+1 Multiplication

Binary Modulo 2^n+1 Multiplication can be implemented duo to Low-High Lemma by Lai [1], which is stated as followings:

$$AB \bmod (2^n+1) = \begin{cases} (AB \bmod 2^n) - (AB \operatorname{div} 2^n) & \text{if } AB \bmod 2^n \geq AB \operatorname{div} 2^n \\ (AB \bmod 2^n) - (AB \operatorname{div} 2^n) + 2^n + 1 & \text{if } AB \bmod 2^n < AB \operatorname{div} 2^n \end{cases}$$

http://ieeexplore.ieee.org/iel5/6910/18613/00858836.pdf?arnumber=858836

两数模$(2^{16}+1)$相乘的可能情况如下：

$$P = \begin{cases} 2^n \cdot Y \bmod (2^n+1) = (-Y) \bmod (2^n+1) = (\overline{Y}+2) \bmod (2^n+1) & if\ X = 2^n \\ 2^n \cdot X \bmod (2^n+1) = (-X) \bmod (2^n+1) = (\overline{X}+2) \bmod (2^n+1) & if\ Y = 2^n \\ 2^n \cdot 2^n \bmod (2^n+1) = 1 & if\ X = Y = 2^n \\ X \cdot Y \bmod (2^n+1) & \text{otherwise} \end{cases}$$

http://www.cqvip.com/QK/98180A/2006002/21840184.html

C_L=ab mod 2^n，C_H=ab / 2^n，$C_0 = \begin{cases} 1, if\ a=b=0 \\ (\overline{b}+2), if\ a=0 \\ (\overline{a}+2), if\ b=0 \\ 0, otherwise \end{cases}$

4. AES，对 state 矩阵的一列 $\begin{bmatrix} 79 \\ ce \\ 93 \\ 7e \end{bmatrix}$ 作列混淆运算， $GF = x^8+x^4+x^3+x+1$ ，系数矩阵为

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

将这一列与系数矩阵在有限域上相乘，$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}\begin{bmatrix} 79 \\ ce \\ 93 \\ 7e \end{bmatrix}=\begin{bmatrix} 57 \\ 2f \\ 08 \\ 2a \end{bmatrix}$（使用有限域上的加法）

Ⅴ保密通讯

1.链路加密的缺点是报文多次加解密造成时延，交换机上出现明文，用户无法控制报文安全性……

2.端到端加密的缺点是不能隐藏通信流量……

Ⅵ公钥密码

1.公钥密码比传统密码更安全，正确吗？

错误。任何加密算法的安全性依赖于密钥的长度和破译密文所需要的计算量。从抗密码分析的角度看，原则上不能说传统密码优于公钥密码，也不能说公钥密码优于传统密码。

2.公钥密码是一种通用的方法，传统密码已经过时，正确吗？

现有的公钥密码方法所需的计算量大，所以取代传统密码似乎不太可能。

3.什么是“陷门单向函数”？

满足下列 3 个条件的函数 f，称为“陷门单向函数”：

⑴给定 x，容易计算 y=f(x)

⑵给定 y，计算 x 使得 y=f(x)很困难

⑶存在“陷门信息”δ；已知 δ 时，给定 y，若对应的 x 存在，容易计算 x 使得 y=f(x)

4.多项式广义欧几里德除法，欧拉定理：略

Ⅶ RSA 算法

1.已知 RSA 加密算法和解密算法，为什么解密结果等于明文？

$$d=e^{-1} mod\ \varphi(n)\rightarrow ed=1 mod\ \varphi(n)$$

素数p、q满足$n=pq$，以及$0<M<n$，有$M^{k\varphi(n)+1}=M^{k(p-1)(q-1)+1}\equiv M\ mod\ n$

$$M^{ed}\equiv M\ mod\ n$$

2.给定 RSA 的密钥参数 p=7,q=13,e=5，求公钥和私钥

n=pq=91

φ(n)=(p-1)(q-1)=72

$d=e^{-1}$ mod φ(n)=29

公钥为{e=5,n=91}，私钥为{d=29,n=91}

3.给定 RSA 公钥{e=5,n=91}，加密 M=62

模重复平方计算法计算 62^5=69 mod 91，密文 D=69

4. RSA-OAEP 对 RSA 的改进是从确定性算法变为概率性算法从而抵抗适应性选择密文攻击，其代价是密文扩张为明文的两倍长度。

Ⅷ ECC

F_q上 ECC 曲线方程 $y^2=x^3+ax+b \bmod q, a, b \in F_q$

椭圆曲线方程 $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ 上，平常点 A(x,y)的切线的斜率 $k=(3x^2+2a_2x+a_4-a_1y)/(2y+a_1x+a3)$ http://tech.csai.cn/web/20060402170453190 6.htm

1. q=23,a=1,b=1，P(17,20)、Q(7,12)，求-P、P+Q、2P

⑴-P=(17,-20)=(17,3)

⑵设过 P、Q 的直线为 y=kx+c，解得 k=10、c=11；根据根与系数关系有 $x_1+x_2+x_3=k^2$ ，解得 x_3=7；-(P+Q)=(7,12)，P+Q=(7,-12)=(7,11)

注意： $x_1+x_2+x_3=k^2$ 这个要记住；使用有限域运算；最后不要忘了取负

⑶设过 P 的切线为 y=kx+c，根据公式求得 k=(3×17²+1)/(2×20)=17/17=1、c=3；根据根与系数关系有 $x_1+x_2+x_3=k^2$ ，解得 x_3=13；-(2P)=(13,1)，2P=(13,-1)=(13,22)

2. ECC 算法的密钥生成方法：选定 Ep(a,b)、K=kG，公钥为{Ep,K,G}、私钥为{Ep,k}；加密算法：明文编码到点 M，产生随机整数 r，计算 C1=M+rK、C2=rG，密文为{C1,C2}。问，解密算法是什么？

M=C1-kC2

Ⅸ散列函数

1.什么是散列函数的单向性？

给定 x，计算 y=H(x)容易；给定 y，求 x 使 y=H(x)困难

2.什么是散列函数的弱抗攻击性？

给定 x，求 y≠x 使得 H(x)=H(y)困难

3.什么是散列函数的强抗攻击性？

寻找任何(x,y)使得 H(x)=H(y)困难

4. MD5 算法分组长度 512bit，输出长度 128bit；SHA1 算法分组长度 512bit，输出长度 160bit

Ⅹ数字签名

RSA 签名方案是 $S=(H(Message))^d \bmod n$

1.如何验证一个 RSA 签名？

若 $S^e \equiv H(Message)(mod\ n)$ ，则报文未被篡改

2.为什么要对 H(Message)签名、而不是 $S=(Message)^d \bmod n$ ？

⑴当 Message 很长，运算量太大

⑵已知 Message 的签名是 S，那么任何人都可以计算 $(Message)^2$ 的签名是 S^2，无法达到来源认证

⑶对 M^e 签名，将导致报文被解密

Ⅺ密钥管理

1.证书至少应包含哪些字段？

所有者的用户名，公钥，证书颁发者对{用户名,公钥}的签名