实验名称：________ 姓名：________ 学号：________

数学基础

整除： $a|b = b=a*k$，a整除b

① $1|a$，若 $a\neq 0$ $a|0$ 且 $a|a$

② $a|b, b|c \Rightarrow a|c$

③ $a|b, a|c \Rightarrow a | s\cdot b+t\cdot c$

$gcd(a,b)=1 \Leftrightarrow$ a,b 互素

裴蜀定理： $gcd(n,u) = an+bu$，特别地当 n,u互素 $an+bu=1$

证明：数学归纳法 ✱，设 $r=n-q*u$

欧几里得算法

若 $a\equiv b \pmod n$，$c\equiv d \pmod n$，则有 $a+c=b+d$，$a-c=b-d$，$ac\equiv bd \pmod n$

装

逆元：

$a+b\equiv 0 \pmod n$，$a*b\equiv 1 \pmod n \Leftrightarrow$ 设a的逆元为b $gcd(a,n)=1 \Leftrightarrow x\cdot a+y\cdot n=1$ （x就是逆元）

将1不断拆解.

订

古典密码:

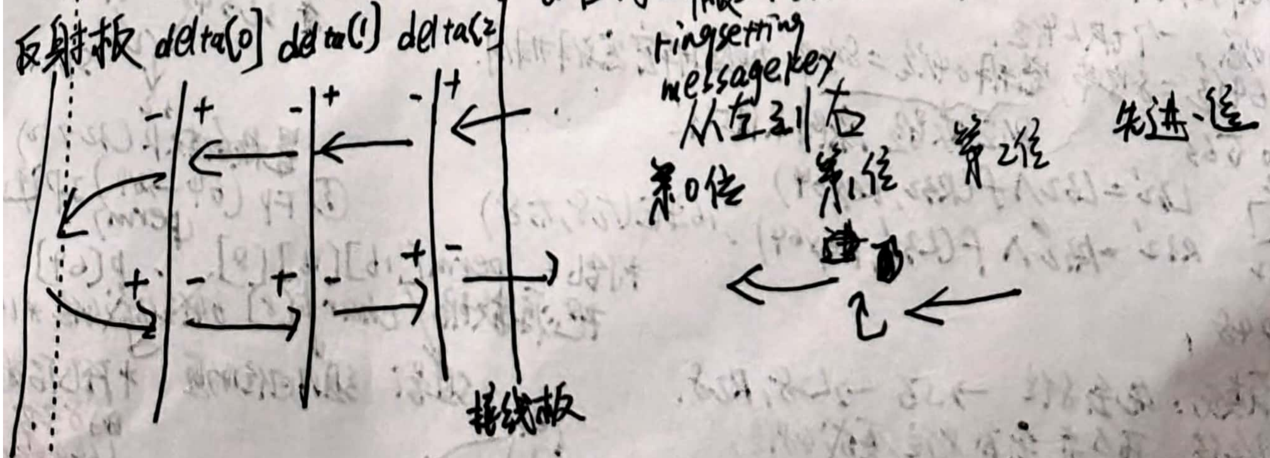
线 加法密码，乘法密码，仿射密码，简单替换密码.

多表密码：playfair，~~vignere~~ vigenere，Hill，Enigma

Enigma: ring setting RFWKA，double setting 中间齿轮特殊情况会转

- message key = △ QEVJZ 假设三个齿轮从左到右分别是 I，II，I

I 从Q→R
II 在前则在E



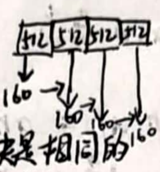
实验名称：______ 姓名：______ 学号：______

md5：无论什么进去，都是 128bit MD5值

分块，每块64字节（512bit），最后一块大小应为 [0,63]，如果是64，则下一块(0)才是最后一块

if (n<56)
  补 (0x80 0x00 ……) 补到56为止（56要大小），再补8个字节，报文长度
else if (n ∈ [56,63]
  补 64-n+56个字节，再补8个字节 = message 总共的位数

hash / SHA-1，结果160位，20字节。 $0 \sim 2^{64}$
分块，每块64字节



分组密码工作 & 流密码

ECB：明 key→ 密，对于相同明文段，加密后的密文块是相同的

CBC：引入种子数 上一个密文作为下一个的种子

$C_j = E_k(P_j \oplus C_{j-1})$，$P_j = D_k(C_j) \oplus C_{j-1}$ 串行 加密时的前一个

装

订

CFB：种子 iv 把种子(密文)去加密，再和明文异或
  e = des(iv, key)
  c[0] = p[0] ^ e[0]
  每次输一次 以左移一位，最右由 c[0] 替代
  种子会变化。
  e = des(iv', key)
  c[1] = p[1] ^ e[0]

线

流密码 rc4：
  state[256]，在 prepare 里打乱初始化
  x, y, buf 无关，和上一次有关

DES：块加密，一个块64位
  明文64位 = 8字节，密钥64位 = 8字节，加密解密密钥相同。
  8位校验，实际只有56位

大端 左0 右63
L32 R32
| 高 | 低 |
R32/L32

L32' = L32 ^ f(R32, key64)
R32' = R32 ^ f(L32', key64)，16轮（左8，右8）

f：32→48

DES 加密：① IP 64→64 perm 表置换
② f (32→32) 16轮
  32→48
  64→48
  sbox
  32
  置换函数 P (32→32)
③ FP (64→64) IP 逆运算 perm

打乱：perm[16][16][8]，p[64]
把源数据 / char p[8] 64位分成4位 * 16组
组号 i 组内四位的值 打乱后的4位的8字节（64里只有4有效）

1011
0001 0001 0001

异或。

再或

key64 每轮有变化：先去8位 →56 →L28, R28。
每轮左移1/2位，再合并，去掉8位，变成48位，
最后两者异或，最后进入 sbox，输出32位就是 f()

sbox[8][64]，共八组，每一组64（4×16），一行16
48分成8组，每组 6→4，各进入8个sbox，

三重 DES：
c = E(D(E
p = D(E(D

比如 101110，第0和第5合并成10为行号，1~4为列号，查表得13，四位输出 1101

实验名称：_____ 姓名：_____ 学号：_____

f (ulong32 r, unsigned char subkey[8]

一共查8次表.

rt 循环移

rval |= sbox [i] [(rt >> 26) ^ *subkey++) & 0x3F];

>> 22

>> 18

>> 14

>> 10

>> 6

>> 2

循环左移

rt ^= *subkey

装 订 线

des_cfb_encrypt (p[], n, des_seed_iv[], des_iv[]

des_seed_key

des_key ~ des_seed_key

des_iv ~ des_seed_iv

while (n > bytes)

{ n -= bytes

memcpy (t, sv, 8)

des_encrypt (t, des_key) ⟶ v = des_encrpt (iv)

memcpy (t+8, p, bytes)

p += bytes

for i=0 i<8

t[i+8] ^= t[i]

memcpy (c, t+8, bytes)

key = seedkey ^ iv ^ seediv

iv = iv << 1 | c[0]

如此

memcpy (t, sv, 8)

c += bytes

if (bits % 8 == 0)

memcpy (t, t + bits/8, 8)

else for (i=0; i<8, i++)

t[i] = t[i + bits/8] << bits%8 | t[i+bits/8+1] >> (8-bits%8)

memcpy (sv, t, 8)

memcpy (iv, t, 8)

存在 y.

$y^2 \equiv x \bmod p \iff x^{(p-1)/2} \equiv 1 \bmod p$

$p>2$ 素, $\gcd(x,p)=1$

① $y^2 \equiv x \bmod p \rightarrow x^{(p-1)/2} \equiv 1 \bmod p$

$\Downarrow$

$\gcd(y,p)=1$

② $x^{(p-1)/2} \equiv 1 \bmod p \rightarrow y^2 \equiv x \bmod p$

设 $x \in Z_p = \{0, 1, \cdots, p-1\}$ 有限域 $Z_p^* = \{1, \cdots, p-1\}$

~~循环群~~ 在模 p 乘法运算下是一个循环群

$\therefore$ 一定存在 Z_p^* 的一个成元 b. St. $x = b^i \bmod p$, $1 \le i \le p-1$

($\because$ 生1)

$\Rightarrow 1 \equiv x^{(p-1)/2} = b^{i(p-1)/2} \bmod p = b^{\frac{(p-1)i}{2}} \bmod p$.

$\because b$ 的阶是 $p-1$ $\therefore b^{(p-1)} \bmod p = 1$ $\therefore i$ 一定是偶数

$\therefore x$ 模 p 的平方根 有整数解 $= b^{\frac{i}{2}} \bmod p$.

装 订 线

实验名称：________ 姓名：________ 学号：________

AES 分组加密

明文=128位=密文长度=16字节

密钥 { 128位 10 / 192位 12 / 256位 14

轮递一下

p[0] p[1] -- p[3]
p[4]
p[12] - - -

→ 8位 [1][2] - - - [16] → p[0] p[1] p[2] p[3]

明文
↓
(和密钥异或)初始变换
↓
9轮循环运算
↓
1轮最终轮
↓ ↓
密文 只做124

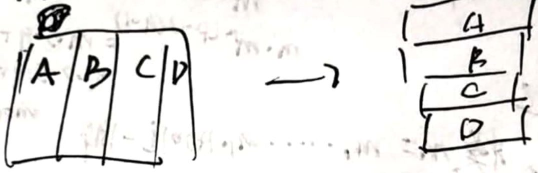
sbox
↑
字节代换 subbytes
明文向左移位 行移位 shiftrow
(左乘矩阵) 列混合 Mix columns
轮密钥加 Addroundkey
和扩展的(每轮)密钥异或

$W[i]=W[i-4] \oplus W[i-1]$

$W[i]=W[i-4] \oplus T(W[i-1])$

Mixcolumn (p, a, 1) 做乘,竖变化

Mixcolumn (p, a, 0) 只做竖变化



按列取

乘法是8位数乘法 mod 0x11B、加法是异或

农夫算法

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

* 低位 4 3 2 1 高位

x3 (3×4 + 3×1 + 1×2 + 2×1)
x2 (1×4 + 1×3 + 2×2 + 3×1)
x1 (1×4 + 2×3 + 3×2 + 1×1)
x0 (2×4 + 3×3 + 1×2 + 1×1) $x^8+x^4+x^3+x+1$

0x11

农夫算法: P是乘积

3 ×3 = 0000 0011 ×0000 0011

当乘数最低位=1时,把被乘数加到p中 (异或)

p = 0000 0011

被乘数左移1位

乘数右移1位

p = 0000 0011 = 0101
0000 0110

EBD9
9EBD
D9EB
BD9E

```
p=0
for (int i=0, i<8, i++)
{
  if (y & 1)
    p ^= x;
  y >>= 1;
  x <<= 1
  if (x & 0x100)
    x ^= 0x11B
}
return p
```

被除

1 0001 1011

if x >= 256. 把它转换成小于等于3次

x^8+1

sbox

x ^= 0x101

7. ecdsa $R=d*G$

$r=(k*G).x \bmod n$

$s=(m+r*d)/k \bmod n$

验证 $((m/s \bmod n)*G+(r/s \bmod n)*R).x \equiv r \pmod n$

$m*G/s + r*R/s = (mG+rdG)/(m+rd)/k$

ecnr $r=((k*G).x+m) \bmod n$

$s=k-r*d \bmod n$

$r \sim (s*G+r*R^P).x \bmod n == m \bmod n$

实验名称：_____ 姓名：_____ 学号：_____

6. RSA

P,q 素，$n=p\cdot q$，n公开，p,q保密 选e 和 $(p-1)*(q-1)$ 互素，

找出d，$e*d=1 \bmod (p-1)(q-1)$，e公钥 d私钥

$c=m^e \bmod n$

$m=c^d \bmod n$

$\varphi(n)$

若 $\gcd(x,n)=1$，$x^{\varphi(n)}=1 \bmod n$

若n为素，$x^{p-1}=1 \bmod p$

中国剩余定理

$m_1, m_2, \dots m_r$ 互素

$x \equiv a_i \pmod{m_i}$，模 $m=m_1\cdots m_r$ 的唯一解

$x=\sum_{i=1}^{r} a_i * M_i * (M_i^{-1} \bmod m_i) \bmod M$

证明：① 证明是解

② 证明唯一解 $x_1=\dots$，$x_2=\dots$，相减，$M|(x_1-x_2)$ 矛盾

证明 设m为明文，c为密文，$c=m^e \bmod n$，证明 $m=c^d \bmod n$

① 条件：$n=pq$，$ed=1 \bmod (p-1)(q-1)$，$c=m^e \bmod n$

② $c^d \bmod n = m^{ed} \bmod n = m\cdot m^{k(p-1)(q-1)} \bmod n = m\cdot m^{\varphi(n)} \bmod n$，$\varphi(n)=\varphi(p)\varphi(q)=(p-1)(q-1)$

1° 若 $\gcd(m,n)=1$

$m^{k(p-1)(q-1)}=s\cdot q+1$

$m\cdot m^{k(p-1)(q-1)}=m\cdot s\cdot q+m=(cp\cdot s\cdot q+m) \bmod n = m$

2° 若 $\gcd(m,n)\neq 1$，则m必为p或q的倍数，设为 $m=cp$

则 $\gcd(m,q)=1$

$m^{\varphi(q)}=1 \bmod q$

$m^{k(p-1)(q-1)}=1 \bmod q$

$m^{k(p-1)}=1 \bmod q$

$M_i=\frac{M}{m_i}$

BN_mod_inverse(tx,tx,n,ctx) $tx=tx^{-1} \bmod n$

BN_set_negative

BN_ucmp(tx,r) (<:1)

若 $\gcd(n_1,n_2)$，$\varphi(n_1\times n_2)=\varphi(n_1)\times\varphi(n_2)$

$\varphi(n)=n*\prod_{p|n}(1-1/p)$

数字签名：A发一封信给B，应用B的公钥加密，

A对签名，应用A的私钥加密。

7. $y^2=x^3+ax+b \pmod p$

a,b,p,G,n=G的阶，素因子，决定了曲线

R公钥点 $=d*G$，d私钥随机数，$d<n$

加密，曲线两加除，$7*(2,7)=(7,2)$

$r=(k*G).x$，k是随机数

$s=m*[(k*R).x] \bmod n$，m是明文

发文包括 r,s

大写是点。

Euler准则 p是素数

若方程有解：$y^2=x \bmod p \Leftrightarrow x^{(p-1)/2}\equiv 1 \pmod p$

opensslE函数

BN_CTX_new()

RSA_size(prsa), RSA_new(), BN_new()

BN_hex2bn(&pn,N)

RSA_public_encrypt(n,bufin,bufout,prsa, RSA_NO_PADDING)

BN_bin2bn(bufin,n,pin)

BN_bn2bin(pout,bufout)

BN_mod_exp(pout,pin,pe,pn,ctx) $pin^{pe} \bmod pn$

EC_GROUP_set_curve_GFP(group,p,a,b,ctx)

EC_GROUP_new() G=EC_POINT_new(group)

EC_POINT_set_affine_coordinate_GFP(group,G,gx,gy,ctx)

EC_GROUP_set_generator(infinity) T=T+G

EC_POINT_Add(group,T,T,G,ctx)

解密

$T=k*G$

$m=s/(d*r).x=m*(k*R).x/(d*(k*G)).x$

求逆

EC_POINT_mul(group,T,m,p,n,ctx) $T=m*G+p*n$

BN_mod_mul(s,m,tx,n,ctx) $s=m\cdot tx \bmod n$

EC_POINT_set_compressed_..._GFP(group,T,r,0,ctx) 求y

证明