密码

1. 广义凯撒密码

令 $m=26$，A,B,$\cdots$,Z 被表为 26 个数 0,1,$\cdots$,25.

Alice 与 Bob 先决定 key(r,s), $0\le r,s\le 25$, 且 $(r,26)=1,(r,s)\ne(1,0)$

Alice 给 Bob 发：

加密：$c\equiv r\cdot m+s\ (mod\ 26)$

解密：$m\equiv r^{-1}(c-s)\ (mod\ 26)$

2. 指数型密钥及 Diffie-Hellman key 交换

原理：取模运算中，指数运算极快，取对数及开方运算极慢

Alice 与 Bob 先决定素数 p，及密钥 k,$(k,p-1)=1$

加密：$c\equiv m^k\ (mod\ p)$

解密：$q\equiv k^{-1}\ (mod\ p-1)$，$m\equiv c^q\ (mod\ p)$

证明：$c\equiv m^k\ (mod\ p)$

由 $kq\equiv 1\ (mod\ p-1)$

得 $kq=l(p-1)+1$

故 $c^q\equiv m^{kq}\equiv m^{l(p-1+1)}\equiv(m^{p-1})^l m\overset{(Fermat)}{\equiv}1^l m\equiv m\ (mod\ p)$

例：$p=29,k=11$

发送明文 $WATER$

转换为数字 $22,0,19,4,17$

加密：$22^{11}\equiv 6\ (mod\ 29)$

$0^{11}\equiv 0\ (mod\ 29)$

$19^{11}\equiv 27\ (mod\ 29)$

$4^{11}\equiv 5\ (mod\ 29)$

$17^{11}\equiv 12\ (mod\ 29)$

c = “6，0，27，5，12”

解密：解 $11 \cdot q \equiv 1\ (mod\ 28)$ 得 $q = 23$

$6^{23} \equiv 22\ (mod\ 29)$

$0^{23} \equiv 0\ (mod\ 29)$

$27^{23} \equiv 19\ (mod\ 29)$

$5^{11} \equiv 4\ (mod\ 29)$

$12^{11} \equiv 17\ (mod\ 29)$

安全性： 对于凯撒密码，若 Eve 知道 m, c，可易得 (r, s)

对于指数密码，若 Eve 知道 m, c，要得到 k，要解 $m^{?} \equiv c\ (mod\ p)$，离散对数问题，难解

· Diffie-Hellman 密钥交换

Alice 与 Bob 选取素数 p，以及数 r，使 $(r, p) = 1, (r, p-1) = 1$

1) Alice 选取数 k_1, 保存

计算 $x_1 \equiv r^{k_1}\ (mod\ p)$，于公共信道发给 Bob

2)Bob 选取数 k_2, 保存

计算 $x_2 \equiv r^{k_2}\ (mod\ p)$，于公共信道发给 Alice

3）Alice 计算 $k \equiv x_2^{k_1}\ (mod\ p)$,Bob 计算 $k \equiv x_1^{k_2}\ (mod\ p)$

由 $x_2^{k_1} \equiv (r^{k_2})^{k_1} \equiv r^{k_1 k_2}\ (mod\ p)$，$x_1^{k_2} \equiv (r^{k_1})^{k_2} \equiv r^{k_1 k_2}\ (mod\ p)$，知其有效可行

例： 两人决定 $p = 23, r = 5$

1) Alice 选 $k_1 = 14$

$x_1 \equiv 5^{14} \equiv 13\ (mod\ 23)$, 将 13 发送

2) Bob 选 $k_2 = 5$

$x_2 \equiv 5^5 \equiv 20\ (mod\ 23)$, 将 20 发送

3)Alice 计算 $20^{14} \equiv 4\ (mod\ 23)$

Bob 计算 $13^5 \equiv 4\ (mod\ 23)$

共享密钥 4

3.RSA 公钥密码体系与数字签名

Bob 想给 Alice 发信息

1)Alice 选取两个大素数 p_A, q_A，计算 $n_A = p_A q_A$

Alice 再选一正整数 e_A，$(e_A, n_A) = 1, (e_A, (p_A - 1)(q_A - 1)) = 1$

Alice 计算 $d_A \equiv e_A^{-1}\ (mod\ (p_A - 1)(q_A - 1))$

Alice 公开 (n_A, e_A)，即公钥

2)(加密)Bob 计算 $c \equiv m^{e_A}\ (mod\ n_A)$

从公共信道发给 Alice

3)(解密)Alice 计算 $m \equiv c^{d_A}\ (mod\ n_A)$

可行性： $n_A = p_A q_A$

$\varphi(n_A) = (p_A - 1)(q_A - 1)$

$e_A \equiv d_A^{-1}\ (mod\ (p_A - 1)(q_A - 1))$

$e_A d_A = l(p_A - 1)(q_A - 1) + 1$

$c \equiv m^{e_A}\ (mod\ n_A)$

$c^{d_A} \equiv m^{e_A d_A} \equiv m^{l(p_A-1)(q_A-1)+1} \equiv (m^{(p_A-1)(q_A-1)})^l m \overset{(Fermat)}{\equiv} 1^l m \equiv m\ (mod\ n_A)$

例： 假设 Bob 要给 Alice 发送 NO(13,14)

1) Alice 选 $p_A = 53, q_A = 71, n_A = 3763, e_A = 11$

计算 $d_A \equiv 11^{-1} \equiv 331\ (mod\ (53-1) \times (71-1))$, 公开 $(3763, 11)$

2) Bob 计算 $c \equiv 1314^{11} \equiv 1265\ (mod\ 3763)$，公开发送

3)Alice 计算 $m \equiv 1265^{331} \equiv 1314\ (mod\ 3763)$

安全性： Eve 需解 $?^{e_A} \equiv c\ (mod\ n_A)$

$e_A \cdot ? \equiv 1\ (mod\ \varphi(n_A))$，这里 n_A 难以分解

若明文可用字母数量太小，可被穷尽 $?^{e_A} \equiv c\ (mod\ n_A)$ 来破解，为了规避这个问题，Alice 与 Bob 可以对 m 施加扰动。如 Bob 要给 Alice 发送 13，他可以发送 1773，2213，1399 等

但 Eve 还可以干扰 Alice 和 Bob 的交流，伪装成 Bob 给 Alice 发信息，因为她知道 (n_A, e_A)

· 数字签名

Bob 要给 Alice 发送带签名的消息

1)Alice 选取两个大素数 p_A, q_A，计算 $n_A = p_A q_A$

Alice 再选一正整数 e_A，$(e_A, p_A q_A (p_A - 1)(q_A - 1)) = 1$

Alice 计算 $d_A \equiv e_A^{-1}\ (mod\ (p_A - 1)(q_A - 1))$

Alice 公开 (n_A, e_A)

2)Bob 选取两个大素数 p_B, q_B，计算 $n_B = p_B q_B$

Bob 再选一正整数 e_B，$(e_B, p_B q_B (p_B - 1)(q_B - 1)) = 1$

Bob 计算 $d_B \equiv e_B^{-1}\ (mod\ (p_B - 1)(q_B - 1))$

Bob 公开 (n_B, e_B)

3)Bob 计算 $c \equiv m^{e_A}\ (mod\ n_A)$

$Sig_B = c^{d_B}\ (mod\ n_B)$

公开发送 (c, Sig_B)

4)Alice 计算 $m \equiv c^{d_A}\ (mod\ n_A)$

5)Alice 验证签名 $c \equiv Sig_B^{e_B}\ (mod\ n_B)$，若成立则消息为 Bob 发送的

可行性： $Sig_B = c^{d_B}\ (mod\ n_B)$

$d_B \equiv e_B^{-1}\ (mod\ (p_B-1)(q_B-1))$

$d_B e_B \equiv l(p_B-1)(q_B-1)+1$

$Sig_B^{e_B} \equiv c^{d_B e_B} \equiv c^{l(p_A-1)(q_A-1)+1} \equiv (c^{(p_A-1)(q_A-1)})^l c \overset{(Fermat)}{\equiv} 1^l c \equiv c\ (mod\ n_B)$

例：假设 Bob 要给 Alice 发送 24

1) Alice 公钥为 $(133,25), 133 = 7\times 19, (25, 7\times 19\times 6\times 18) = 1$
Bob 公钥为 $(143,7), 143 = 11\times 13, (7, 11\times 13\times 10\times 12) = 1$

2) Alice 私钥为 $13 \equiv 25^{-1}\ (mod\ 6\times 18)$
Bob 私钥为 $103 \equiv 7^{-1}\ (mod\ 10\times 12)$

3)Bob 计算 $c \equiv 24^{25} \equiv 73\ (mod\ 133)$
$Sig_B \equiv 73^{103} \equiv 57\ (mod\ 143)$
发送 $(73, 57)$

4)Alice 计算 $24 \equiv 73^{13}\ (mod\ 133)$，得到信息

5)Alice 验证签名 $73 \equiv 57^7\ (mod\ 143)$，匹配，得知信息的确来源于 Bob