总复习. 6月10日.

一. 机密性服务: 加密方案 Encryption Scheme.

3个算法
① 密钥生成
② 加密
③ 解密

3个空间
① 密钥空间
② 明文~
③ 密文~.

3个角色: 加密方、解密方、攻击者(敌手)、完全控制信道。

二. 古典加密: 移位密码、单表替换.

三. 现代对称加密: DES的基本事实: key length. 轮数. 4种工作模式 如 CBC. ECB.
代码 Festel结构.

四. 公钥密码算法/协议.

1. 历史. DH'76 协议. RSA'78. ElGamal '86.

p, $\mathbb{Z}_p^* = \{1, \cdots, p-1\}$. 乘法 Group.

g 生成元. $\langle g \rangle = G$.

$g^{x \in \mathbb{Z}_p^*}$

B.g. $y \in \mathbb{Z}_p^*$.

$X = g^x \pmod p$. $Y = g^y$.

x →
← Y

$K_A = Y^x = g^{xy}$ $K_B = X^y = g^{xy}$

攻击者 $(p, g, X, Y) \not\to g^{xy}$ DH问题.

模幂运算. 平方-乘 手工计算

2. RSA PKE.

① KeyGen. p, q, $N=pq$. $\varphi(N)=(p-1)(q-1)$.

$$ed \equiv 1 \pmod{\varphi(N)}$$

先选定 e，再此式求 d，$(d=e^{-1} \bmod \varphi(N))$

$(e, \varphi(N))=1$

"互素 ⇔ 存在逆元"

利用扩展欧几里得算法求.

$\gcd(a,b)=aX+bY$

⇓

$1=eX+Y\varphi(N)$.

$\Rightarrow eX=1-Y\varphi(N)$.

$\Rightarrow eX \bmod \varphi(N) = (1-Y\varphi(N)) \bmod \varphi(N)$

$\equiv 1 \bmod \varphi(N) - 0$.

$\Rightarrow eX \equiv 1 \pmod{\varphi(N)}$

$\Rightarrow d=X$

② 加密算法：$c=m^e \pmod N$

"平方-乘"

③ 解密~：$m=c^d \pmod N$

(CRT 是降计算不作要求)

数论：整除. 全数. $a=kb+r$

同余. gcd. 线性组合. $q=3$

剩余集(剩余类).

$\mathbb{Z}_n$: 完全剩余集

	0	1	2	3	4	$p=5$
0	0	6	12	3	9	
1	10	1	7	13	4	
2	5	11	2	8	14	

q

$\mathbb{Z}_{15} \leftrightarrow \mathbb{Z}_5 \times \mathbb{Z}_3$

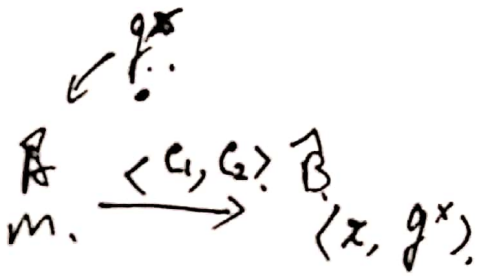
$\{0, \dots 14\}$

3. ElGamal PKE. (基于DH协议).

① KeyGen: 选 p, $\mathbb{Z}_p^*$, g.

私钥: $x \in \mathbb{Z}_{p-1}$.

公钥: g^x.



② 加密

a) 选 $r \in \mathbb{Z}_{p-1}$.

计 $g^r = c_1$.

b) 计算 $(g^x)^r = k$.

$c_2 = m \cdot k$.

$\langle c_1, c_2 \rangle$

③ 解密:

a) 先计 k: $k = c_1^x = g^{rx}$

b) 求 m, $m = c_2 \cdot k^{-1}$.

4. PKI: 基本概念.

公钥证书: 组成, 生成, CA

使用. (首先要确认证书有效) (基本含义)

5. DS: 基本概念.

$h = H(m)$. $\sigma = Sign(h, sk)$.

$Verify(h, PK) = \begin{cases} 0: N \\ 1: Y \end{cases}$

6. Hash函数. 基本性质

: ····防碰撞····