计网hw chapter 8　武雅涵　2012202.

R5. 输入块：2^8种输入（256种）

映射：256！种映射

密钥：256！

R6. 对称密钥：$C_N^2 = \binom{N}{2} = \frac{N(N-1)}{2}$

公开密钥：每个人生成一个属于自己的公钥公开发布，保留私钥

任意发起一次通信 A→B 都可以用B的公钥加密 $K_B^+(m)$，B用保留的私钥解密 $K_B^-(K_B^+(m)) = m$.

共需2N个密钥。

R15. 我认为基于数字签名的方案更适合。

采用MAC的方式需要向"数以千计"的请求者分发一个鉴别密钥，首先分发的代价可能很高，其次将有很多用户共享鉴别密钥安全性难以保障。但如果同每个用户发不同的密钥，代价将很昂贵。

采用数字签名的方案只需要在互联网上发布同一的相同的公钥，分发代价更低，也无需损害安全性。

R23. Bob使用Alice的公钥加密（前）主密钥发送给Trudy，Trudy无法解析出对称密钥

在握手算法最后，~~Bob向~~ Trudy向Bob发送一个包括所有~~之~~前握手报文的MAC. Bob验证失效，拒绝连接.

P3.

不可以.

因为采用了多码代替密码，加密采用了多个单码(分别包含不同的映射信息)，并且还包含了这些单码使用的顺次序信息，这取选择文本只能确保每个字母出现至少一次，不足以破解加密方式。

P7. $p=3$ $q=11$ $n=pq=33$ $z=2\times10=20$

选择 $e=3$ e和z互素 选择 $d=7$

$21 \bmod 20 = 1$

$k^+:(33,3)$ $k^-(33,7)$

加

密文c.	cd.	$m=c^d \bmod n$
d 4.	16384	16
o 15.	17085375	
g 7	823543	

解

明文c	c^e	密文 $m=c^{de} \bmod n$	解密 $m^d \bmod n$.
d 4	16384	16	
o 15	17085375	27	
g 7	823543	28	

明文c.	c^e (e=3)	$c^e \bmod n$ 密文m	m^d	$m^d \bmod n$	
d 4	64	3	2 | 512614111	4	d
o 15	3375	9	4 | 82969	15	o
g 7	343	13	62 | 4851	7	g

b) d: 00100

o: 01111 → dog: 00100 01111 00111

g: 00111

明文 m = 4583

因为 $c = (m^e \bmod n)^d \bmod n = m$. 故 m 应小于 n.

因为自己确实没有能力找到一组这么大的RSA公钥，上网学习搜索到

p = 43 q = 107 n = p × q = 4601 z = 4452

e = 61 d = 73

$m^e \bmod n = 4602 = c$ $c^d \bmod n = 4583 = m$.

P8. a $n = pq = 5 \times 11 = 55$

$z = (p-1) \times (q-1) = 4 \times 10 = 40$

b. 因为 $e = 3 < n = 55$，e 和 z 互素、

并且通常选择较短的公钥

c. 选择 d = 67 $e \times d = 240 \equiv 1 \bmod z = 1$

d. 密文 $c = 8^3 \bmod 55 = 17$

pg. a. ~~$T_A = S_A \bmod p$ $T_B = S_B \bmod p$~~

$T_A = S_A^g \bmod p$

$T_B = S_B^g \bmod p$

$S = S_A^{T_B} \bmod p = S_A^{(S_B^g \bmod p)} \bmod p$

$S' = S_B^{T_A} \bmod p = S_B^{(S_A^g \bmod p)} \bmod p$

又有 $(a \bmod n)^d \bmod n = a^d \bmod n$.

$S = (S_A \bmod p)^{S_B^g \bmod p} \bmod p = (S_A \bmod p)^{(S_B \bmod p)^g \bmod p} \bmod p$

$S' = (S_B \bmod p)^{S_A^g \bmod p} \bmod p = (S_B \bmod p)^{(S_A \bmod p)^g \bmod p} \bmod p$

$T_A = g^{S_A} \bmod p \quad T_B = g^{S_B} \bmod p$

$S = T_B^{S_A} \bmod p = g^{S_A S_B} \bmod (g^{S_B} \bmod p)^{S_A} \bmod p = (g^{S_A S_B} \bmod p) \bmod p$

$S' = T_A^{S_B} \bmod p = (g^{S_A} \bmod p)^{S_B} \bmod p = (g^{S_A S_B} \bmod p) \bmod p$

$S = S'$

b). $T_A = S_A^g \bmod p = 5^2 \bmod 11 = 25 \bmod 11 = 3$

$T_B = S_B^g \bmod p = 12^2 \bmod 11 = 1.$

c) $S = S_A^{T_B} \bmod p = 5^1 \bmod 11 = 5$

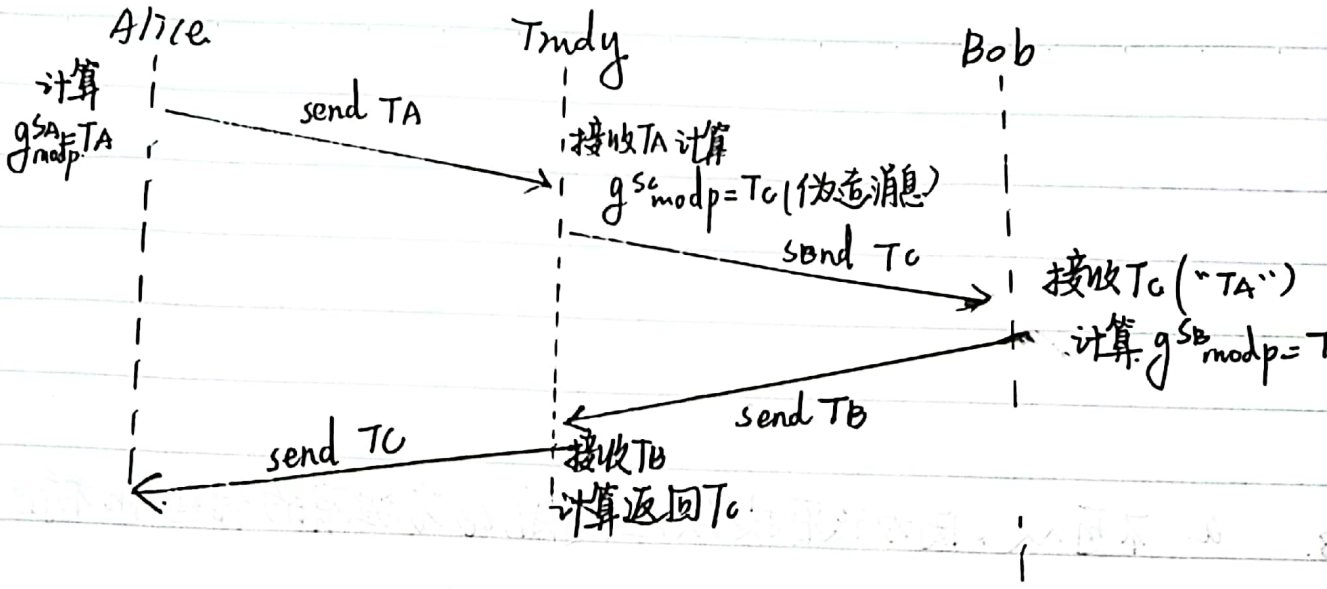
$S' = S_B^{T_A} \bmod p = 12^3 \bmod 11 = 1.$

~~d)~~ b). $T_A = g^{S_A} \bmod p = 2^5 \bmod 11 = 10$

$T_B = g^{S_B} \bmod p = 2^{12} \bmod 11 = 4$

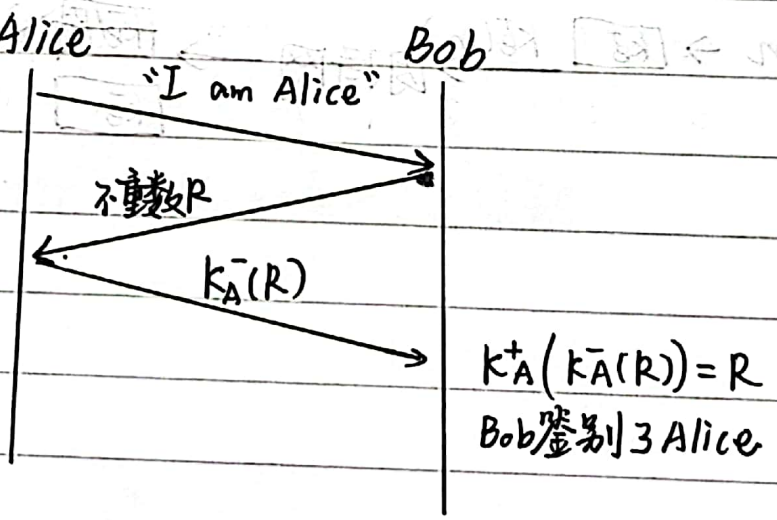
c). $S = (g^{S_A S_B} \bmod p) \bmod p = 2^{40} \bmod 11 = 1$

d).



Trudy分别和Alice/Bob各得到一个仅两方可知的共享密钥S. 可以截获报文

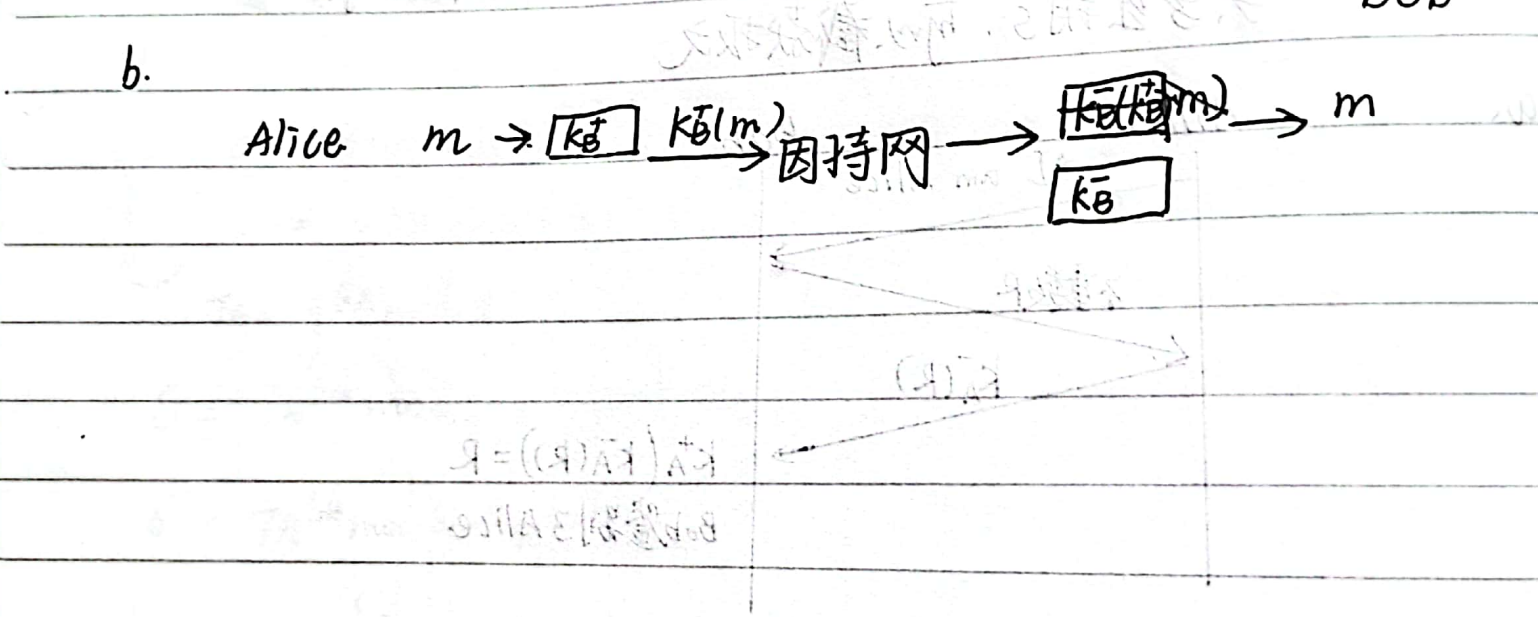
P16. a.



b. Alice向Bob分发公钥的报文被Trudy拦截，Trudy向Bob发送自己的公钥 K_T^+ 并声称"I am Alice"，之后Trudy收到Bob发送的不重数R，用 K_T^- 加密后发送给Bob，Bob解码后认为认证成功。同样Trudy也可以欺骗Alice声称"Bob"就可以获知甚至修改它们通信的内容了。

P18. a. 不可以，因为没有提供任何Alice方独有的信息和标志。

b.



P19 a. 客户

b. 128: IP地址：216.75.194.220
端口号：443.

c. 204+79 = 283.

d 3

e. 它会用server 公钥加密的3个密钥

f. bc. 29.

g 客户端：发送3：3条 接收3：3条
共6条.

h. 服务器端：发送3 4条 接收3 3条
共7条