16th Week

Chapter 8

R5. 2^8个输入块，$2^8!$种映射，$2^8!$种可能的密钥.

R6. 总共需要 $\frac{N(N-1)}{2}$ 个密钥；使用公共密钥需要 $2N$ 个.

R15. 对于MAC，Alice 要与每个可能的接收方建立共享密钥；对于数字签名，则对每个接收方使用相同的数字签名。由题意基于数字签名更合适.

R23. 客户端生成预主密钥PMS后，将用Alice对其加密公钥，将加密的PMS发给Trudy. Trudy 无法解密PMS，因此没有私钥，也不能确定共享的认证密钥。在握手的最后一步中，他向Bob发送所有握手消息的MAC，使用随机的验证密钥；当Bob接收MAC，MAC测试失败，Bob将结束TCP连接.

P3. 该报文中的句子中包含了所有26个字母，因此在选定的明文攻击中，凯撒密码将了解每个明文字符的密文字符，但是Vigenere密码不总是将给定明文字符转换为相同的密文字符，因此Vigenere密码不会被立刻打破.

P7. a) 对于RSA，由 $p=3$，$q=11$ 得 $n=33$，$q=11$，选择 $e=9$，$d=9$：（注：**表示乘方）

加密：	d	letter	m	m**e	ciphertext = m**e mod 33
		d	4	262144	25
		o	15	38443359375	3
		g	7	40353607	19

解密：	ciphertext	c**d	m = c**d mod n	letter
	25	3814697265625	4	d
	3	19683	15	o
	19	322687697779	7	g

b) 过程类似于a，此时 $p=43$，$q=107$，$n=p*q=4601$，$z=(p-1)(q-1)=4452$，$e=61$，$d=73$.

P8. a) $n = p*q = 55$ $\quad \beta = (p-1)(q-1) = 40$

b) e小于n且与β没有公因子.

c) $d = 27$

d) $m = 8$, $m^e = 512$, Ciphertext $c = m^e \bmod n = 17$.

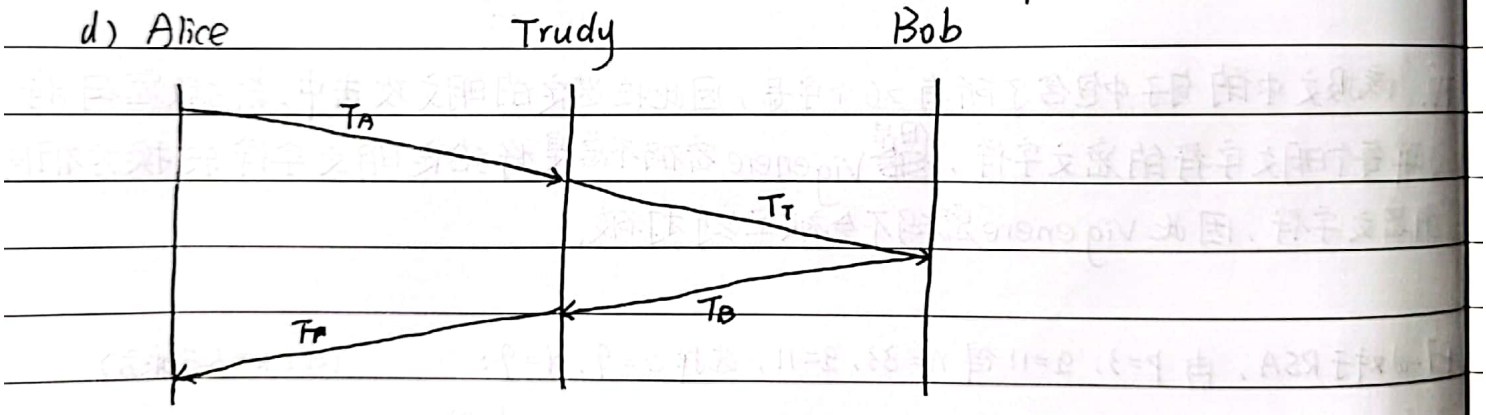
P9. a) $S = (TB^{SA}) \bmod p = ((g^{SB} \bmod p)^{SA}) \bmod p = (g^{SB\,SA}) \bmod p$

$= ((g^{SA} \bmod p)^{SB}) \bmod p = (TA^{SB}) \bmod p = S'$

b) and c) $p = 11$, $g = 2$.

	Alice	Bob
密钥	$S_A = 5$	$S_B = 12$
公钥	$T_A = (g^{SA}) \bmod p = 10$	$T_B = (g^{SB}) \bmod p = 4$
共享密钥	$S = (T_B^{SA}) \bmod p = 1$	$S' = (T_A^{SB}) \bmod p = 1$

d)



P16. 无法解决此问题，因为Bob不正确地认为自己在前半部对Alice进行认证，而Alice可能误认为在认证Bob，主要由于Bob和Alice都可以认为他们得到的公钥是自己的.

P18. a) 没有这样的方案，因为没有公钥/私钥对或预共享密钥，Bob无法验证Alice发了消息

b) 可以，Alice使用Bob的公钥对消息进行加密并发给Bob.

P19. a) 客户端

b) IP: 216.75.194.220 端口: 443

c) 283

d) 3个 SSL 记录

e) 正确的，包含了一个加密的主密钥.

f). bc 和 29

g) 6个 (?)