第六章

Problem 6

Suppose that wireless station H1 has 1000 long frames to transmit. (H1 may be an AP that is forwarding an MP3 to some other wireless station.) Suppose initially H1 is the only station that wants to transmit, but that while half-way through transmitting its first frame, H2 wants to transmit a frame. For simplicity, also suppose every station can hear every other station's signal (that is, no hidden terminals). Before transmitting, H2 will sense that the channel is busy, and therefore choose a random backoff value.

Now suppose that after sending its first frame, H1 returns to step 1; that is, it waits a short period of times (DIFS) and then starts to transmit the second frame. H1's second frame will then be transmitted while H2 is stuck in backoff, waiting for an idle channel. Thus, H1 should get to transmit all of its 1000 frames before H2 has a chance to access the channel. On the other hand, if H1 goes to step 2 after transmitting a frame, then it too chooses a random backoff value, thereby giving a fair chance to H2. Thus, fairness was the rationale behind this design choice.

Problem 8

a) 1 message/ 2 slots
b) 2 messages/slot
c) 1 message/slot

a) i) 1 message/slot
ii) 2 messages/slot
iii) 2 messages/slot

b) i) 1 message/4 slots
ii) slot 1: Message A→ B, message D→ C
slot 2: Ack B→ A
slot 3: Ack C→ D
= 2 messages/ 3 slots

iii)
slot 1: Message C→ D
slot 2: Ack D→C, message A→ B
slot 3: Ack B→ A
Repeat

= 2 messages/3 slots

第八章

Problem 7

a) We are given $p = 3$ and $q = 11.$ We thus have $n = 33$ and $q = 11.$ Choose $e = 9$ (it might be a good idea to give students a hint that 9 is a good value to choose, since the resulting calculations are less likely to run into numerical stability problems than other choices for $e.$) since 3 and $(p-1)*(q-1) = 20$ have no common factors. Choose $d = 9$ also so that $e*d = 81$ and thus $e*d-1 = 80$ is exactly divisible by 20. We can now perform the RSA encryption and decryption using $n = 33$, $e = 9$ and $d = 9.$

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

ciphertext	c**d	m = c**d mod n	letter
25	38146972265625	4	d
3	19683	15	o
19	322687697779	7	g

We first consider each letter as a 5-bit number: 00100, 01111, 00111. Now we concatenate each letter to get 001000111100111 and encrypt the resulting decimal number m=4583. The concatenated decimal number m (= 4583) is larger than current n (= 33). We need m < n. So we use p = 43, q = 107, n = p*q = 4601, z = (p-1)(q-1) = 4452. e = 61, d = 73

ciphertext = m**e mod 4601

m**e= 21386577601828057804089602156530567188611499869029788733808438804302864595620613956725840720949764845640956118784875246785033236197777129730258961756918400292048632806197527785447791567255101894492820972508185769802881718983

ciphertext = m**e mod 4601 = 402

c**d
= 1283813313619771634195712132539793287643533147482536209328405262
7930271588610123920532872496335709674931222802214538150129342413705402045814598714979387232141014703227794586499817945633390592

ciphertext = m**e mod 4601 = 4583

Problem 9

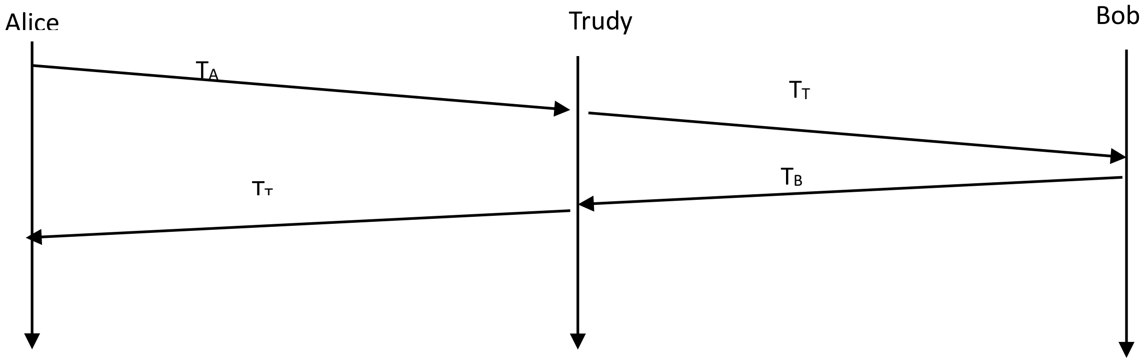
	Alice	Bob
secrect key:	S_A	S_B
public key:	$T_A = (g\text{^}S_A) \bmod p$	$T_B = (g\text{^}S_B) \bmod p$
shared key:	$S = (T_B\text{^}S_A) \bmod p$	$S' = (T_A\text{^}S_B) \bmod p$

a) S = (TB^SA) mod p = ((g^SB mod p)^SA) mod p = (g^(SBSA)) mod p
= ((g^SA mod p)^SB) mod p = (TA^SB) mod p = S'

(b and c) p = 11, g = 2

	Alice	Bob
secrect key:	$S_A= 5$	$S_B = 12$
public key:	$T_A = (g\text{^}S_A) \bmod p = 10$	$T_B = (g\text{^}S_B) \bmod p = 4$
shared key:	$S = (T_B\text{^}S_A) \bmod p = 1$	$S' = (T_A\text{^}S_B) \bmod p = 1$

d)

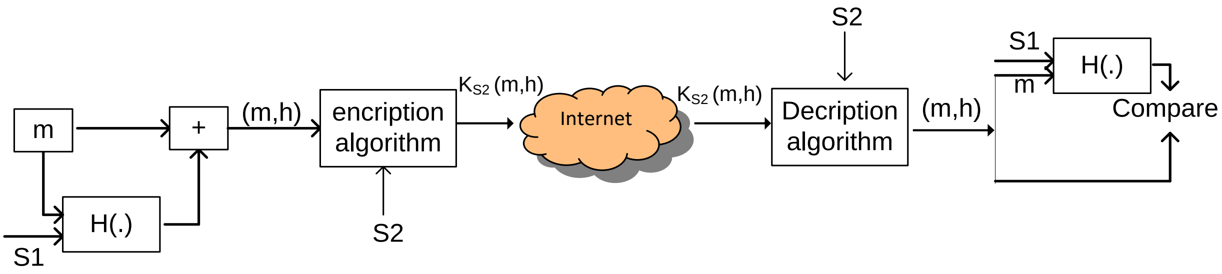


The Diffie-Hellman public key encryption algorithm is possible to be attacked by man-in-the-middle.

1. In this attack, Trudy receives Alice's public value (T_A) and sends her own public value (T_T) to Bob.
2. When Bob transmits his public value (T_B), Trudy sends her public key to Alice (T_T).

3. Trudy and Alice thus agree on one shared key (S_{AT}) and Trudy and Bob agree on another shared key (S_{BT}).
4. After this exchange, Trudy simply decrypts any messages sent out by Alice or Bob by the public keys S_{AT} and S_{BT}.

Problem 12


m
+
H(.)
S1
(m,h)
encription algorithm
S2
K_S2 (m,h)
Internet
K_S2 (m,h)
S2
Decription algorithm
(m,h)
S1
m
H(.)
Compare