NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Information Security and Communication Technology

Examination paper for TTM4135 Information security

Academic contact during examination: Colin Boyd

Phone: 73551758

Examination date: 2017-05-19

Examination time (from-to): 09:00 - 12:00

Permitted examination support material: (D) No printed or hand-written support material is allowed. A specific basic calculator is allowed.

Other information: –

Language: English

Number of pages: 2

Number of pages enclosed: 0

Checked by:

Date Signature

TTM4135 August exam 2017:
Outline answers

Exercise 1 Multiple choice questions

1.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
2.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
3.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
4.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
5.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
6.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
7.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
8.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
9.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
10.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
11.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
12.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
13.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
14.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
15.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
16.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
17.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
18.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
19.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
20.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
21.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
22.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
23.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
24.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
25.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
26.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
27.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
28.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
29.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
30.	(a) ☑	(b) ☐	(c) ☐	(d) ☐

Exercise 2 Written answer questions

1. (a) For the simple substitution there are 27! keys. For the transposition cipher there are 10! keys

   (b) For the simple substitution, a chosen plaintext attack will allow the substitution for each letter to be obtained by making the plaintext equal to the alphabet, so only 27 letters are required. For the transposition, the whole key can be obtained from a single block as long as a chosen plaintext of 10 different characters is used. (Strictly speaking we only need to see 9 of these.)

2. (a) The receiver must recompute the tag exactly as done by the sender (actually only needs to see the last two blocks) and compare it with the one that was sent.

   (b) The problem is that the tag only depends on P_{t-1} and P_t. Thus given a long message, all blocks can be changed except for the last two, and the same tag remains valid.

3. (a) Only need check that $2^6 \bmod 13 \neq 1$ and $2^4 \bmod 13 \neq 1$. $2^4 \bmod 13 = 3$ and $2^6 \bmod 13 = 12$. Thus 2 is a generator.

   $3^3 = 27 \bmod 13$ so 3 has order 3 so 3 is not a generator

   (b) The secret is $z = g^{ab} = y^a = 8^3 \bmod 13 = -8 \bmod 13 = 5$

4. (a) Since $s = h(m)^d \bmod n$ for a valid signature, the verifier must compute $s^e \bmod n$, compute $h(m)$ and check that they are equal.

   (b) Now $s = m^d \bmod n$. An attacker can choose a random value for s and then compute $m = s^e \bmod n$. Then s is a valid signature for the random message m (existential forgery).

5. (a) ID_B is used to tell A who the key is going to be shared with by S. If it were omitted an adversary could masquerade as B by changing the identity ID_B going to A in message 1 and A would not see any change.

   (b) An attacker who controls B's clock can make B accept an old timestamp. This allows a replay attack in which the attacker replays an old message 3. Since we assume that the attacker can obtain old session keys it will then be able to continue the communication and masquerade as A.

6. (a) i. To protect your email contents you need to use PGP, since STARTTLS only provides link encryption.

   ii. To protect mail headers PGP does nothing, but STARTTLS can do this, at least against outside parties, since it encapsulates whole message within TLS.

   (b) PGP uses a web of trust approach to certificates which allows any party to act as a certifier. TLS uses X.509 hierarchical certification authorities.