NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Telematics

Examination paper for TTM4135 Information security

Academic contact during examination: Colin Boyd

Phone: 73551758

Examination date: 2016-08-18

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 2016: 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) ☐

Exercise 2 Written answer questions

1. (a)

$$\begin{aligned} C &= KP \\ &= \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 2 & 0 \end{pmatrix} \end{aligned}$$

   (b)

$$\begin{aligned} K^{-1} &= 4^{-1} \begin{pmatrix} 2 & -2 \\ -2 & 4 \end{pmatrix} \bmod 5 \\ &= 4 \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \end{aligned}$$

   (c)

$$\begin{aligned} P &= K^{-1}C \\ &= \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 3 & 2 \end{pmatrix} \end{aligned}$$

2. (a) $P_t = D(C_t, K) \oplus C_{t-1}$
   (b) From the encryption equation we see that encryption requires the previous ciphertext block. So parallel encryption is not possible.
   (c) From part (a) we see that decryption only uses ciphertext blocks which are already received. Therefore parallel decryption is possible.
   (d) If one bit is flipped in one ciphertext block, say C_t, we see from the decryption equation that this affects two decrypted blocks, P_t and P_{t+1}. For P_t we can expect a random change in all bits, but for P_{t+1} only the position of the bit flip in C_t will be changed.

3. (a) $M = s/r^x \bmod p$ where $y = g^x$.
   (b) Suppose the attacker knows that M_1 is the plaintext for $C_1 = (r_1, s_1)$. Then he obtains $y^k = s_1/M_1$. For any other ciphertext $C_2 = (r_2, s_2)$ he can then obtain $M_2 = s_2/y^k$.

4. $M_p = C^{17 \bmod 4} \bmod 5 = 2^1 \bmod 5 = 2$
   $M_q = C^{17 \bmod 6} \bmod 7 = 2^5 \bmod 7 = 4$
   $M = (2 \times 7 \times 7^{-1} \bmod 5) + (4 \times 5 \times 5^{-1} \bmod 7) = (14 \times 3) + (20 \times 3) \bmod 35 = 32.$

5. (a) The recipient must share the key K and so can recompute the tag T for the received message M. If this agrees with the received tag then the message is accepted as authentic.
   (b) Given M and T the attacker computes $H(K) = T \oplus H(M)$. Then $T' = H(M') \oplus H(K)$ can easily be computed by the attacker.

6. (a) The ticket contains the key $K_{C,V}$ from the ticket granting service so the purpose is to allow V to obtain and to verify the authenticity and freshness of this shared key. The authenticator is generated by C to convince V that C is currently active (entity authentication).
   (b) On receipt of the second message C should decrypt and check that the timestamp is still current. Since V is the only other party which possesses $K_{C,V}$ it is the only party who could have formed a correct second message.

7. (a) The advantage of using elliptic curves compared with using groups $\mathbb{Z}_p^*$ is that the keys and public key (Diffie-Hellman values) can be shorter for the same security level.
   (b) Only with ephemeral Diffie–Hellman values can forward secrecy be obtained. Static DH uses long-term keys which, if revealed, give away the DH shared secret.
   (c) ECDSA signatures are used to authenticate the ephemeral Diffie–Hellman values exchanged in the handshake protocol.
   (d) User data is authenticated using GCM mode which has a built-in authentication check.