TTM4135 August exam 2018:
Outline answers

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) □

2 Written answer questions

1. (a) For the Vigenère cipher there are 27^{10} keys. For the simple transposition there are 10! keys.

   (b) For the Vigenère cipher a chosen plaintext attack will reveal the shift of each character since the difference, mod 27, between the plaintext and ciphertext character is the key character. Thus with just 10 known plaintext/ciphertext pairs the key can be found. The same information is given with a known plaintext attack.

   For the simple transposition a plaintext with 10 different characters is sufficient to find the permutation. Thus a chosen plaintext attack will give the key by choosing 10 different characters. A known plaintext attack might leave some ambiguity after 10 characters if some of them are the same, so more plaintext/ciphertext pairs may be needed.

2. (a) The receiver recomputes that tag using the received IV and the message to find the CBC ciphertext. The receiver then checks that the last block is equal to the received T.

   (b) We have $C_1 = E(P_1 \oplus IV, K)$. An attacker can replace P_1 with any message block P' by also replacing IV with $IV' = IV \oplus P_1 \oplus P'$. Then the value of T is unchanged and can be sent with the IV' as the MAC tag.

3. (a) $d = e^{-1} \bmod \phi(n) = 3^{-1} \bmod \phi(55) = 3^{-1} \bmod 40 = 27$.

   (b) The attacker simply computes the greatest common divisor of each pair of moduli to efficiently find the shared prime. This can be computed efficiently using the Euclidean algorithm. Once one prime factor is known ordinary division can be used to find the other prime.

4. (a)

$$\begin{aligned} 2^8 \bmod 17 &= 1 \\ 3^8 \bmod 17 &= -1 \end{aligned}$$

   Thus the order of $g = 2$ is 8 or less, while the order of 3 is 16, so 3 is a generator.

   (b) We need to find the value x such that $3^x \bmod 17 = 5$.

i	$3^x \bmod 17$
1	3
2	9
3	10
4	13
5	5
…	…

   Thus $\log_{17} 5 = 5$.

5. - $K_{C,tgs}$ is a shared key to be used with the next server (ticket granting server or TGS). It needs to be included to enable secure communication with the next server.
   - ID_C is the identity of the client, which is used so that the TGS knows who the key is shared with. If it were not included the ticket then a malicious C could masquerade as a different party.

- T_1 is an expiry date (or timestamp) to ensure that the ticket is fresh. If it were not included then the ticket could be re-used at a later time, which could allow an old $K_{C,tgs}$ session key to be re-used.

6. (a) The client sends available ciphersuites and version number in the client hello message. The server replies with its preferred (strongest) matching versions.

   (b) Advantages (any two):

   - Allows for better interoperability between clients and servers who may be using older versions with weaker ciphersuites
   - Allows the client and server to find the most secure cipher suite they both support.
   - Versatility should any particular (fixed) cipher suite be broken. It's then trivial to change to another suite without changing the protocol.

   (c) All of the handshake messages are authenticated in the finished messages, ensuring that the negotiation message (hello messages) are authentic.