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: 2018-06-04

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: 3

Number of pages enclosed: 0

Checked by:

Date Signature

TTM4135 Spring exam 2018:
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) In a chosen plaintext attack the attacker can choose a plaintext (matrix P for the Hill cipher) and see the corresponding ciphertext (matrix C for the Hill cipher. In a chosen ciphertext attack the attacker can choose a ciphertext and see the corresponding plaintext.

   (b) The attacker can choose $P = I$ (identity matrix) and is then given the key as C. (Also acceptable to choose any invertible P, obtain C and compute $K = CP^{-1}$.)

   (c) Yes, a chosen ciphertext will also work, choosing C to be invertible and then $K = CP^{-1}$

2. (a) If the IV is fixed then the encryption is deterministic. This means that the same plaintext results in the came ciphertext, allowing dictionary attacks.

   (b) With a chosen plaintext attack, the attacker simply asks for the encryption of any message with first block equal to P_1. If the first ciphertext block output is the same as in the captured ciphertext then the captured ciphertext has first block equal to P_1

3. (a) $e = d^{-1} \bmod \phi(n) = 5^{-1} \bmod \phi(21) = 5^{-1} \bmod 12 = 5$.
   $c = 3^5 \bmod 21 = 54 \bmod 21 = 12$.

   (b) From her own e_A and d_A values, A can factorise n using Miller's algorithm. Then she can compute d_B from e_B and $\phi(n)$ in the usual way.

4. (a)

$$\begin{aligned} 2^4 \bmod 13 &= 3 \\ 2^6 \bmod 13 &= 12 \end{aligned}$$

   Thus the order of $g = 2$ must be 12, so it is a generator.

   (b) A sends $2^a = 3$ so $a = 4$. So the shared secret is $6^4 \bmod 13 = 10^2 \bmod 13 = 9$.

5. (a)

$$\begin{aligned} g^s &= g^{km+xr} \\ &= g^{km} g^{xr} \\ &= r^m y^r \end{aligned}$$

   Note that due to Fermat's theorem, exponents which are equal modulo $p - 1$ are equivalent.

   (b) We will get two different s values with the same k and so same r. The same x is always used. Only unknowns are x and k.

$$\begin{aligned} s_1 &= (km_1 + xr) \bmod (p-1) \\ s_2 &= (km_2 + xr) \bmod (p-1) \end{aligned}$$

   $s_1 - s_2 = k(m_1 - m_2) \bmod (p-1)$ so k can be found. The equation is easily solved as long as $(m_1 - m_2)$ has an inverse. Thus a few different m_1 and m_2 values may need to be tried. Then $xr \bmod (p-1)$ can also be found. Thus an attacker can reuse r and compute $s = (km + xr) \bmod (p-1)$ for any other m value.

6. (a) The first ciphersuite uses ephemeral Diffie-Hellman authenticated by ECDSA signatures. This provides forward secrecy since the long-term keys are used only for authentication. The second ciphersuite uses key transport with the RSA key of the server used to protect the master secret chosen by the client. It does not provide forward secrecy since if the server long-term decryption key is revealed the pre-master secret can be decrypted.

   (b) The first ciphersuite uses GCM which provides authenticated encryption. SHA-256 is used in the key derivation. (The hash used within the GCM algorithm does not use SHA-256.) The second ciphersuite uses 3-DES for encryption and SHA-1 for HMAC construction. These are algorithms with lower security level than those used in the first ciphersuite. More specifically, 3DES has 112 bit security while AES has 128 bit security. SHA-1 has been broken and deprecated and should not be used.