TTM4135 exam May 2021: Outline answers

1 Multiple choice questions

1. Suppose that $x^{-1} \bmod 17 = 5$. Then

   (a) $x \bmod 17 = 7$

   (b) $x \bmod 17 = 6$

   (c) $x \bmod 17 = 5$

   Explanation:

2. Suppose that the 26-letter alphabet, $A \ldots Z$ is used for the plaintext in the 2×2 Hill cipher. Suppose that the letter E is the most common letter in the plaintext, occuring with frequency equal to 10%. Then in the ciphertext we can expect that:

   (a) the most common letter occurs with frequency equal to 10%

   (b) the most common letter occurs with frequency below 10%

   (c) the most common letter occurs with frequency above 10%

   Explanation:

3. A typical RSA private key in use today may have length 3072 bits, but a typical symmetric key for the AES block cipher may have length only 128 bits. This longer key for RSA is necessary because:

   (a) security for public key encryption needs to be stronger than for symmetric key encryption

   (b) RSA keys need to be longer than symmetric keys to avoid attack by quantum computers

   (c) there are much better ways to attack RSA than brute force key search

   Explanation:

4. Suppose that in a binary synchronous stream cipher a section of the ciphertext is 01000. An attacker knows that the plaintext used to obtain this ciphertext is 00101. The corresponding section of the decryption keystream is:

   (a) 01101

   (b) 00101

   (c) 01000

Explanation:

5. Consider the version of the triple DES (3-DES) block cipher with three independent keys. Compared with the AES block cipher, this version of 3-DES:

   (a) has fewer possible keys than all versions of AES

   (b) has a shorter block length than all versions of AES

   (c) is faster to run in software than all versions of AES

   Explanation:

6. Suppose that you have a message of 100 bits to encrypt and you choose to use the AES block cipher. Which of the following modes of operation will require the least number of sent bits in the encrypted message?

   (a) ECB mode

   (b) Counter mode with a nonce of 64 bits

   (c) CBC mode

   Explanation:

7. The Euler function ϕ is often useful for public key cryptography. It is true that:

   (a) $\phi(n)$ is always divisible by 3

   (b) if n is divisible by 3 then $\phi(n)$ is always divisible by 3

   (c) if n is divisible by 9 then $\phi(n)$ is always divisible by 3

   Explanation:

8. Suppose you want to prevent an attacker from finding a collision in a hash function. The attacker has enough computing power to calculate 2^{40} hash values. You need to ensure that the attacker has only small chance of success but prefer the smallest acceptable output size. You have three possible output sizes to choose from. Which should you choose?

   (a) 40 bits

   (b) 64 bits

   (c) 128 bits

   Explanation:

9. A message authentication code, MAC, takes as input a key K and message M and outputs a tag T. In order to be secure, it is essential that:

   (a) an attacker who knows a valid M and T cannot find K

   (b) an attacker who knows a valid K and T cannot find M

   (c) an attacker who knows a valid K and M cannot find T

Explanation:

10. The RSA signature scheme uses a modulus n and a public exponent e. If the modulus is chosen to be $n = 13 \times 23 = 299$ (**corrected**) then the smallest valid choice for e would be

    (a) $e = 3$

    (b) $e = 5$

    (c) $e = 7$

Explanation:

11. For efficiency reasons it is often useful to keep fixed parameter values for many users of a cryptographic scheme. Which of the following is *not* a practical choice for digital signatures?

    (a) RSA signatures with a fixed modulus n

    (b) DSA signatures with fixed generator g and fixed modulus p

    (c) ECDSA signatures with a fixed elliptic curve group

Explanation:

12. When assessing the security of a key establishment protocol, such as the Needham–Schroeder protocol, we assume that an attacker is able to:

    (a) re-send messages sent in any previous runs of the protocol

    (b) force parties to re-use nonces used in previous runs of the protocol

    (c) obtain long-term keys used in any previous runs of the protocol

Explanation:

13. In the TLS 1.2 handshake protocol, a ciphersuite is negotiated between the client and the server. Which of the following does *not* depend on the chosen ciphersuite:

    (a) the algorithm used to authenticate the record layer data

    (b) the algorithm used to sign the server key exchange message

    (c) the algorithm used to sign the server certificate

Explanation:

14. TLS 1.3 aims to establish secure connections faster than TLS 1.2. One difference between the protocols which contributes to this is:

    (a) clients can send a Diffie–Hellman ephemeral value before the ciphersuite is agreed

    (b) checking of server certificates is no longer required

    (c) servers can initiate the handshake protocol and use a ciphersuite of their choice

Explanation:

15. PGP is a security protocol to protect emails in transit. PGP has seen very limited usage in practice. One of the reasons for this is:

    (a) usability is a challenge for many potential users

    (b) encryption is provided but it is not possible to authenticate mail senders

    (c) PGP-encrypted mail cannot be sent on the normal email system

    Explanation:

2 Written answer questions

1. Suppose that you share a new (unused) random key of 128-bits with a recipient. You are considering whether to use the key either as a one-time pad or with the AES block cipher in ECB mode.

   (a) Suppose first that you have a single message to encrypt, written in English as 16 × 8-bit bytes to make 128 bits in total. For this part assume that the key is used only once for this message. Compare the security of each of the two choices. Is one better than the other and why?

   (b) Now suppose that you have a second message to encrypt, also written in English as 16 × 8-bit bytes. You decide to use the same encryption method with the same key as you used for the first 128-bit message. Again, compare the security of the two choices.

2. The Feistel construction for a block cipher uses the round equations:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i) \end{aligned}$$

   for some function f. Suppose that f is chosen to be the function:

$$f(R, K) = R \oplus K$$

   for any half-block, R, and any round key, K.

   (a) Show that with this choice of f it follows that for all $i \geq 2$, both of the following equations hold.

$$\begin{aligned} R_i &= L_{i-2} \oplus K_{i-1} \oplus K_i \\ L_i &= L_{i-2} \oplus R_{i-2} \oplus K_{i-1} \end{aligned}$$

   (b) Use the above observation to show how to break a 2-round Feistel cipher with this f function given one known plaintext/ciphertext pair.

   (c) Explain, just giving the idea, how part (ii) can be generalised to break a Feistel cipher with any even number of rounds if this f function is used.

3. One non-trivial square root of 1 modulo 209 is 153.

   Alternate question:

   One non-trivial square root of 1 modulo 221 is 118.

   (a) What are all four of the square roots of 1 modulo 209?

   Alternate question:

   What are all four of the square roots of 1 modulo 221?

(b) Choose one of your non-trivial square roots, x and show, using the Euclidean algorithm, that $\gcd(x+1, 209) > 1$.

So $\gcd(57, 209) = 19$ which is a divisor of 209

Alternate question:

Choose one of your non-trivial square roots, x and show, using the Euclidean algorirhm, that $\gcd(x+1, 221) > 1$.

(c) Explain how an efficient algorithm to find non-trivial square roots can be used to break the RSA cryptosystem.

4. The normal RSA cryptosystem uses modulus $n = pq$, a decryption exponent, d, and public exponent, e. Suppose that a company wants to protect its private exponent so that no single entity can decrypt. The manager splits d into two parts, d_1, d_2 such that

$$d_1 + d_2 \bmod \phi(n) = d.$$

In order to decrypt a ciphertext C, entity E_1 computes $M_1 = C^{d_1} \bmod n$, entity E_2 computes $M_2 = C^{d_2} \bmod n$ and these are combined to form $M = M_1 \times M_2 \bmod n$.

Alternate question:

The normal RSA cryptosystem uses modulus $n = pq$, a decryption exponent, d, and public exponent, e. Suppose that a company wants to protect its private exponent so that no single entity can decrypt. The manager splits d into two parts, d_1, d_2 such that

$$d_1 \times d_2 \bmod \phi(n) = d.$$

In order to decrypt a ciphertext C, entity E_1 computes $M_1 = C^{d_1} \bmod n$, entity E_2 computes $M = M_1^{d_2} \bmod n$.

(a) Show that a ciphertext encrypted with normal RSA, with public key e and n, is decrypted properly with this method. (You may assume that normal RSA works correctly.)

(b) This system runs slower than normal RSA. To improve the efficiency the manager decides to give both E_1 and E_2 the values p and q so that they can use the CRT to decrypt.

i. Does this make the system as fast as normal RSA? Explain your answer.

ii. Why does this defeat the purpose of the system?

5. Consider the following protocol with the goal of key establishment. This is a repaired version of the Needham–Schroeder protocol.

Here N_A is a nonce chosen by party A, N_B is a nonce chosen by B, and K_{AB} is the session key chosen by server S. ID_A and ID_B are identity strings for A and B respectively. K_{AS} and K_{BS} are key-encrypting keys initially shared between S and A, and between S and B respectively. The notation $\{X\}_K$ denotes authenticated encryption of X with key K.

1. $A \to B : ID_A, N_A$
2. $B \to S : ID_A, ID_B, N_A, N_B$
3. $S \to B : \{N_A, ID_A, ID_B, K_{AB}\}_{K_{AS}}, \{N_B, ID_A, ID_B, K_{AB}\}_{K_{BS}}$
4. $B \to A : \{N_A, ID_A, ID_B, K_{AB}\}_{K_{AS}}$

(a) On receipt of message 4, A should check that the received N_A is the same value as that chosen in message 1. Describe an attack on the protocol if A does not perform this check, including the messages which an attacker sends. What is the consequence of this attack?

(b) On receipt of message 3, B should also check that the received ID_A is the same identity received in message 1 and sent in message 2. Describe an attack if B does not perform this check.

Alternate question:

(b) Suppose that instead of using authenticated encryption, plain encryption by a synchronous stream cipher is used, such as AES in counter mode. How does this also allow an attack?

6. The Signal messaging protocol uses two kinds of *ratcheting* to update the keys used to protect messages: Diffie–Hellman ratcheting is used when the next message is sent in the opposite direction from the previous message; symmetric ratcheting with a hash function is used when the next message is sent in the same direction. Assume a powerful adversary who can capture and delay messages and has the ability to compromise devices later.

   (a) How does the ratcheting in Signal improve the security of messages against this adversary, in comparison to the security of:

      i. email messages encrypted with PGP;

      ii. messages sent as application data in a TLS 1.3 session.

   (b) If several messages are sent in the same direction in the Signal protocol, how does their security compare to the security of messages sent successively in opposite directions?