TTM4135 exam August 2021: Outline answers

1 Multiple choice questions

1 point for correct answer, 0.5 point penalty for incorrect answer. Explanation can say why one answer is correct, **or** why two answers are wrong for 1 point. Possible to get 0.5 point for explanation of why one answer is wrong.

1. Suppose that $3x = kn + 1$ for positive integers x, k and n. Then it follows that:

   (a) $3^{-1} \bmod n = x \bmod n$ ✓

   (b) $3^{-1} \bmod n = k \bmod n$

   (c) $3^{-1} \bmod k = n \bmod k$

   Explanation: $3x \bmod n = kn + 1 \bmod n = 1$

2. Two historical ciphers are the simple substitution cipher and the Vigenère cipher. Suppose that the 26-letter alphabet, $A \ldots Z$ is used for the plaintext and that the Vigenère cipher has a key of length 5. Which of the following is true?

   (a) The Vigenère ciphertext will most likely have a flatter (more uniform) frequency distribution than the simple substitution ciphertext ✓

   (b) The Vigenère cipher has more possible keys than the simple substitution cipher

   (c) The most frequent character in the Vigenère ciphertext will most likely be same as the most frequent character in the simple substitution ciphertext

   Explanation: The Vigenére cipher substitutes each plaintext character with different ciphertext characters resulting in a flatter distribution, in contrast to the simple substitution cipher which preserves the letter frequencies.

3. Suppose that in a binary synchronous stream cipher a section of the keystream is 01101. An attacker knows this keystream and intercepts the corresponding ciphertext 00101. The corresponding section of the plaintext is:

   (a) 01000 ✓

   (b) 00101

   (c) 01101

Explanation: Since $C = P \oplus K$ we can also calculate $P = K \oplus C = 01101 \oplus 00101 = 01000$.

4. The DES block cipher and the AES block cipher differ in the following way:

   (a) AES has only one round function but DES uses several different round functions

   (b) AES has only one S-box but DES uses several different S-boxes ✓

   (c) AES has only one round key but DES uses several different round keys

Explanation: Both AES and DES are iterated ciphers with different round keys and a fixed round function. AES has only one large S-box.

5. Suppose that you have a message of 160 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: ECB uses two 128-bit blocks so 256 bits; counter mode uses 160 bits + 64 bits for nonce so 224 bits; CBC uses two 128 ciphertext blocks and 128 bits for IV so 384 bits.

6. Suppose you want to prevent an attacker from finding a collision in a hash function. The attacker has enough computing power to calculate 2^{80} hash values. You need to ensure that the attacker has only a small chance of success but you prefer the smallest acceptable output size. You have three possible output sizes to choose from. Which should you choose?

   (a) 128 bits

   (b) 256 bits ✓

   (c) 384 bits

Explanation: Due to the birthday paradox, with 2^{80} trials there is a good chance of a collision being found with an output of length 160 bits. Therefore more than 160 bits is necessary.

7. A message authentication code, MAC, takes as input a key K and message M and outputs a tag T. Suppose an attacker observes a valid tag T for a known message M. In order to be secure, it is essential that:

   (a) the attacker cannot find a valid T for the same M and a different K

   (b) the attacker cannot find a valid M for the same T and a different K

(c) the attacker cannot find a valid T for the same K and a different M ✓

Explanation: Finding a new valid T with the same K is a forgery. For a different K the attacker can choose the key so this is not a forgery.

8. The Euler function ϕ is often useful for public key cryptography. Suppose that $n = 143 = 11 \times 13$. Then for any a, it is true that:

   (a) $a^{150} \equiv a^{30} \bmod n$ ✓

   (b) $a^{150} \equiv a^{8} \bmod n$

   (c) $a^{150} \equiv a^{15} \bmod n$

Explanation: $\phi(n) = 120$ so by Euler $a^x \bmod n = a^{x+120} \bmod n$.

9. A typical RSA private key in use today may have length 3072 bits, but a typical elliptic curve private key may have length around 256 bits. This longer key for RSA is necessary because:

   (a) security for RSA encryption needs to be stronger than for elliptic curve encryption (such as ElGamal encryption on elliptic curves)

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

   (c) there are faster algorithms known to solve the factorisation problem than there are to find elliptic curve discrete logarithms ✓

Explanation: Factorisation has sub-exponential time algorithms, but we only know exponential time algorithms for the EC discrete logarithm problem.

10. Consider the following encryption scheme, which is similar to, but different from, the ElGamal encryption scheme. A ciphertext for message m has two parts: $C_1 = m \cdot g^k \bmod p$ and $C_2 = y^k \bmod p$, where $y = g^x$ is the recipient public key. In order to recover the message, the recipient must compute $z = x^{-1} \bmod (p-1)$ and then:

    (a) $m = C_1 \cdot (C_2^z)^{-1} \bmod p$ ✓

    (b) $m = C_2 \cdot (C_1^z)^{-1} \bmod p$

    (c) $m = C_1^z \cdot (C_2)^{-1} \bmod p$

Explanation: $C_2^z \bmod p = y^{kz} \bmod p = g^{xkx^{-1} \bmod (p-1)} \bmod p = g^k \bmod p$. Therefore $C_1 \cdot (C_2^z)^{-1} \bmod p = m \cdot g^k \bmod p / g^k \bmod p = m$.

11. The RSA signature scheme often uses a public exponent $e = 2^{16} + 1$. Instead we could try to use a private exponent $d = 2^{16} + 1$ to increase the speed of signature generation. This would not be a good idea because:

    (a) it would not be possible to find the correct public exponent e
    (b) an attacker could easily forge signatures ✓
    (c) the Chinese Remainder Theorem could no longer be used to increase the speed of signature generation

Explanation: If it is know that a fixed d is used, then with the modulus (part of the public key) forging signatures is trivial.

12. The Kerberos V5 security protocol provides authentication and key establishment using an online authentication server (AS) which shares a long-term key with each user. A limitation this protocol is:

    (a) forward secrecy is not provided ✓
    (b) an attack is possible involving replay of a previously used session key
    (c) users need to obtain certified public keys in order to use the protocol

Explanation: If a user long-term key is compromised then tickets from the AS can be decrypted to obtain the key used. So forward secrecy is not provided. The attack on Needham–Schroeder is not valid on Kerberos due to the use of timestamps in tickets. Public keys are not used.

13. When TLS is used to protect web browser communications with HTTPS, a set of root certificates comes with the browser. The keys from these root certificates are used to:

    (a) verify server certificates sent in the TLS handshake protocol ✓
    (b) sign Diffie-Hellman ephemeral keys used in the TLS handshake protocol
    (c) encrypt the pre-master secret sent in the TLS handshake protocol

Explanation: The root certificates are the root of security (authenticity) so that the signatures in server certificates can be verified. The server public key is used for signing Diffie-Hellman shares or, in the RSA case for TLS 1.2, encrypt the pre-master secret.

14. In typical usage of tunnel mode, the IPSec protocol provides:

    (a) protection of user metadata ✓
    (b) end-to-end security of user data
    (c) non-repudiation of user data

Explanation: IPSec in tunnel mode is typically used for gateway-to-gateway architectures. The original IP header is encapsulated in a new IP packet and hidden from eavesdroppers.

15. PGP is a security protocol to protect emails in transit. One limitation of PGP is:

    (a) a corrupted mail server is able to read the contents of PGP-encrypted mail

    (b) a corrupted mail server can reveal the metadata such as sender and recipient identities ✓

    (c) a corrupted mail server can forge valid PGP signatures on behalf of any message sender

Explanation: PGP provides end-to-end security but must leave headers intact to allow routing of the message.

2 Written answer questions

1. Consider the following version of the historical Vigenère cipher. The alphabet consists of 64 characters (for example, 52 lower and upper case letters, 10 digits, full stop and comma). Encryption of each plaintext character p_i consists of a shift defined by a key character k_i. The key K is specified by a sequence of 20 characters: $K = k_0 \dots k_{19}$ where k_i for $i = 0, \dots, 19$ gives the amount of shift in the ith alphabet, i.e.

$$c_i = p_i + k_{i \bmod 20} \bmod 64.$$

   (a) How many possible keys does this cipher have?

   (b) By comparing with the AES block cipher, explain how secure this cipher would be against brute force key search.

   (c) Explain how this cipher is easily broken with a known plaintext attack. Include an estimate of how much known plaintext would be needed.

   (a) There are 64 possible shifts for each key character, so in total there are 64^{20}.

   (b) The number of possible keys is 2^{120} which is equivalent to a 120-bit key, only 8 bits smaller than AES-128 keys. Therefore this cipher is reasonably secure against brute force key search attack .

   (c) With a known plaintext attack, an attacker can see the amount of shift for each key position. The whole key can be recovered from 20 consecutive characters of known/chosen plaintext.

2. Consider a non-standard mode of operation for block ciphers, similar to, but different from, CTR mode. It has the following general equation for computing each output block:

$$C_t = O_t \oplus P_t$$

   where $O_t = E(T_t \oplus C_{t-1}, K)$ and $T_t = N \| t$ is the concatenation of a nonce N and block number t, and $C_0 = 0$ (the block of all 0 bits).

   (a) What is the equation for decryption of ciphertext block C_t to obtain the plaintext block P_t?

   $P_t = C_t \oplus O_t$. (Note that no decryption is required.)

   (b) Suppose that there is an error in transmission when block C_t is sent to a recipient, so that one bit is changed. How many blocks, or partial blocks, are changed when the receiver decrypts? Explain your answer.

   One bit change in C_t will change one bit in the decrypted P_t and change O_{t+1} to be a random block. Thus the next block P_{t+1} will be decrypted as a random block. However, assuming C_{t+1} is correct, O_{t+2} will be correct again and so all following blocks are not affected. Thus only one plaintext block has one bit changed and the following plaintext block is changed to random.

   (c) Is it possible to encrypt multiple plaintext blocks in parallel? Is it possible to decrypt multiple blocks in parallel? Explain your answers.

   To encrypt in parallel you need to have the previous C_{t-1} block so parallel encryption is not possible.
   To decrypt in parallel you already have the previous C_{t-1} block so parallel decryption is possible.

3. A message authentication code (MAC) takes an input message M and key K and computes a tag T. Consider a MAC defined using a block cipher decryption function D with a 128-bit shared key K:

$$\text{MAC}(M, K) = T = D(M, K).$$

This MAC is only defined for messages of exactly 128 bits in length.

(a) Explain how this MAC should be verified by a recipient of a pair (M, T).

The recipient simply recomputes the tag and checks that its computation is the same as the received T. For this MAC the recipient can also encrypt the tag and check that this yields the received message.

(b) Explain why it should be difficult for an attacker to find a valid tag for a given message M, even after seeing many valid message/tag pairs (M_i, T_i) for a fixed K and messages M_i different from M.

To find a valid tag, the attacker needs to decrypt the "ciphertext" M with key K. This should not be possible for a good block cipher. Moreover, a good block cipher should be still be secure given many ciphertext plaintext pairs, which correspond to the (M_i, T_i) pairs.

(c) Suppose that the MAC is now re-defined to allow any message of 256-bits by dividing the 256-bit input M into two 128-bit sub-blocks M_1, M_2 and defining $T = D(M_1 \oplus M_2, K)$. Explain why it is now easy for an attacker to find a forgery given just one valid pair (M, T)

A message M is now two 128-bit blocks, M_1, M_2. But given any such message, the tag T will remain the same by replacing these with M_1', M_2' where $M_1 \oplus M_2 = M_1' \oplus M_2'$. Thus an attacker can choose any M_1' and compute $M_2' = M_1' \oplus M_1 \oplus M_2$ and then the tag T is valid for this new message.

4. The Miller–Rabin algorithm is often used for generation of prime numbers in public key cryptography. A related, but simpler, algorithm is known at the Fermat test. These two tests are compared in this question. Show your working for the computations, which should all be straightforward without use of a calculator.

(a) Show that $2^{10} \bmod 341 = 1$ and deduce that 32 is a non-trivial square root of 1 modulo 341. Use this result to find a factor of 341.

$2^{10} \bmod 341 = 1024 \bmod 341 = 3 \times 341 + 1 \bmod 341 = 1$. Therefore $2^{10} \bmod 341 = (32)^2 \bmod 341 = 1$ and since 32 is different from 1 and -1 it is a non-trivial square root. $\gcd(31, 341)$ must be a factor of 341. 341 = 11*31. (Alternatively, $\gcd(33, 341)$ must be a factor of 341. 341 = 11*31.)

(b) Show that the Fermat test will decide that 341 is a probable prime when the base is chosen as 2.

The Fermat test will compute: $2^{340} \bmod 341 = (2^{10})^{34} \bmod 341 = 1$ so the Fermat test is passed.

(c) Show that the Miller–Rabin test correctly identifies 2 as a composite number.

Since $340 = 85 \times 2^2$, the Miller–Rabin test will compute: $2^{85} \bmod 341 = (2^{10})^8 \times 2^5 \bmod 341 = 32$ and then $32^2 \bmod 341 = 1$. So the M-R test finds the non-trivial square root 32 and identifies 341 as composite.

5. Two digital signature algorithms often used in network security protocols are: RSA signatures and DSA signatures. Suppose that these signatures both use a modulus of size 3072 bits.

Alternate question: Suppose that these signatures both use a modulus of size 4096 bits.

(a) What are the total sizes of the public information needed to verify a signature from each of the two schemes? Show separately the sizes of all different components, including all of the public parameters that would be needed in order to complete the verification.

(b) Suppose that signatures from many different signers will be verified so that some parameters may be shared between different signers. For each of the two signature schemes, state which public parameters cannot be shared and explain why they cannot. What is the size of the public key components that must be different for each signer?

(a) RSA: modulus n: 3072 bits; verification exponent e: 17 bits or random 3072 bits. Total 3089 bits or 6144
DSA: modulus p: 3072 bits; generator g: 3072 bits; public key y: 3072 bits. Total 9216 bits.

(b) RSA modulus cannot be fixed, but public exponent can be fixed. 3072 bits for each user. DSA can fix p and g. 3072 bits for each user.

6. The following ciphersuite for TLS 1.2 is classified as *weak* (for example by SSL Labs):

TLS_RSA_WITH_AES_256_GCM_SHA384

Alternate question: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

This question concerns comparison with the following TLS 1.3 ciphersuite:

TLS_AES_128_GCM_SHA256

(a) Compare the security of these two ciphersuites, commenting on each of the algorithms used for handshake and for record layer security. Why is the TLS 1.2 ciphersuite weak while the TLS 1.3 ciphersuite is not?

In the handshake protocol TLS1.3 ciphersuites always use ECDHE which gives forward secrecy. Using RSA in the handshake does not provide forward secrecy which is why it is classified as weak. The record layer algorithms are actually stronger in the TLS 1.2 ciphersuite since they used longer key lengths.

Alternate answer: In the handshake protocol TLS1.3 ciphersuites always use ECDHE so in fact both ciphersuites specify the same handshake algorithms. which is why it is classified as weak. The record layer algorithms are the same in the TLS 1.2 and TLS 1.3 ciphersuites but the key derivation functions for the TLS 1.2 ciphersuite will use SHA which has been broken (collisions found) which is why it is classified as weak.

(b) How will the security of these two ciphersuites be affected if quantum computers become available to attackers in the future? Is there a difference between the security of sessions which happen *before* the attackers have the quantum computer and those which happen afterwards?

Quantum computers will allow breaking of both factorisation and ECDLP problems, so both ciphersuites will be broken. It does not matter much whether the session

happens before or after quantum computers become available, except that attackers will need to record and store the TLS protocol messages for those session of interest. So storage is required for sessions before quantum computers exist.