TTM4135 Spring exam 2020

1 Multiple choice questions

1. Suppose that n is any odd number. Then $2^{-1} \bmod n$ is:

   (a) $n - 2$
   (b) $(n + 1)/2$
   (c) $(n - 1)/2$

   Explanation:

2. Suppose a plaintext comes from a natural language, similar to English, where the most frequent character appears with probability 1/10. For which of the following ciphers is the frequency of all ciphertext characters likely to be less than 1 in 10?

   (a) The random simple substitution cipher
   (b) A transposition cipher on blocks of size 12
   (c) The Vigenére cipher with a key of length 8

   Explanation:

3. Which of the following ciphers has the largest number of possible keys?

   (a) The triple-DES cipher with two independent keys
   (b) The random simple substitution cipher with alphabet consisting of all 8-bit bytes
   (c) The AES block cipher with the shortest allowed key length

   Explanation:

4. A block cipher is a function $E(m, k)$ which takes a plaintext block m and a key k to a ciphertext block c. In any useful block cipher:

   (a) for a fixed key k, the function $E(\cdot, k)$ is a permutation of the set of plaintext blocks
   (b) for a fixed plaintext block m, the function $E(m, \cdot)$ is a permutation of the set of keys
   (c) for a fixed ciphertext block c, there is a unique pair (m, k) such that $E(m, k) = c$

Explanation:

5. Suppose the string `ABCDE` is a portion of a ciphertext which has been encrypted with the one time pad. The corresponding plaintext string P is another 5-character string. Which of the following is the most accurate statement?

   (a) Every possible plaintext string of length 5 is equally likely to be the correct P

   (b) The attacker gains nothing useful about the correct P from seeing `ABCDE`

   (c) The correct P is the same plaintext corresponding to any previous portion of ciphertext equal to `ABCDE`

Explanation:

6. The discrete logarithm problem in $\mathbb{Z}_p^*$ is the basis for many public key cryptosystems. On conventional computers (not quantum computers) there is:

   (a) no known polynomial time algorithm

   (b) no known subexponential time algorithm

   (c) no known exponential time algorithm

Explanation:

7. The security of RSA encryption is related to the problem of integer factorisation in the following way:

   (a) if RSA cannot be broken then factorisation is hard

   (b) if RSA can be broken then factorisation is easy

   (c) If RSA is secure then factorisation may be easy or hard

Explanation:

8. The RSA encryption algorithm uses a public exponent e, a private exponent d, and a public modulus n. In order to speed up the decryption process, it is common to:

   (a) choose a small value for e

   (b) choose a small value for d

   (c) apply the Chinese Remainder theorem

Explanation:

9. ElGamal encryption works in $\mathbb{Z}_p^*$. The ciphertext of a message m is a pair (g^k, my^k). To avoid a known plaintext attack it is essential to:

   (a) choose a new k for each encryption

   (b) choose a new y for each encryption

   (c) choose a new g for each encryption

Explanation:

10. Let h be the identity function, $h(x) = x$ defined on bit strings of length 128-bits. This function does not meet the property of being:

    (a) oneway
    (b) collision-resistant
    (c) second pre-image resistant

Explanation:

11. HMAC is a takes as input a key K and message M and outputs a tag T. Suppose that HMAC uses the hash function is SHA-256. If $HMAC(K, M_i)$ is computed for many different messages M_i (and a fixed K) then two identical tags will probably first appear after:

    (a) 2^{16} tag values are computed
    (b) 2^{128} tag values are computed
    (c) 2^{255} tag values are computed

Explanation:

12. A difference between a message authentication code (MAC) and a digital signature scheme is:

    (a) a signature must be randomised but a MAC tag need not be
    (b) a MAC tag can be recomputed by the verifier but a signature cannot be
    (c) a MAC provides data integrity but a signature does not

Explanation:

13. The Kerberos protocol makes use of a ticket containing four values $(K_{AB}, ID_A, ID_S, N_A)$ which is shared between a client A and server S. A suitable algorithm to use to protect these values would be:

    (a) AES in GCM mode
    (b) AES in CBC mode
    (c) HMAC

Explanation:

14. A difference between TLS 1.3 and TLS 1.2 is:

    (a) the TLS 1.3 handshake protocol always provides forward secrecy
    (b) there are no known attacks on the TLS 1.3 protocol
    (c) the TLS 1.3 record protocol includes data compression

Explanation:

15. Many email servers add a DomainKeys Identified Mail (DKIM) digital signature to outgoing mail. This signature:

    (a) can be verified by any recipient of the email

    (b) is verified and then removed by the receiving domain mail server

    (c) can only be verified by the receiving domain

Explanation:

2 Written answer questions

1. Consider a variant of the Hill cipher which has the encryption equation

$$C = KP + L \bmod n$$

where the key has two parts, a 2×2 matrix K and 2×1 column vector L. The column vectors C and P represent the ciphertext and plaintext respectively. Here n is the size of the alphabet in use. In this question all matrices are 2×2. If $L = 0$ then this variant is the same as the basic Hill cipher.

   (a) What is the decryption equation for this variant cipher?

   (b) What is the possible number of keys in this variant? Write an expression in terms of n and the number of keys of the basic Hill cipher.

   (c) Explain how an attacker can use a chosen plaintext attack to obtain the key with three chosen plaintext pairs.

2. A non-standard mode of operation for block ciphers has the following general equation for computing each output block: $C_t = E(P_t \oplus P_{t-1} \oplus C_{t-1}, K)$ where $C_0 = IV$ which is sent with the ciphertext and $P_0 = 0$ (the block of all 0 bits).

   Alternate question:
   $C_t = E(P_t \oplus C_{t-1}, K) \oplus P_{t-1}$

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

   (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.

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

3. Two efficient tests for primality of an integer n are the Fermat test and the Miller–Rabin test. Both tests use a base value a chosen randomly in the range $1 < a < n - 1$ and are usually run for multiple bases. Suppose that the tests are being used to test $n = 45$.

   (a) Show that $19^2 \bmod 45 = 1$.

(b) Show that the Fermat test will return that $n = 45$ is a probable prime if the value $a = 8$ is chosen.

(c) Show that the Miller-Rabin test will return that $n = 45$ is composite if the value $a = 4$ is chosen.

4. Consider the Diffie–Hellman protocol in the group $\mathbb{Z}_p^*$. In order to add authentication to the basic Diffie–Hellman protocol it is common to use digital signatures. An alternative is to use a long-term key directly in the protocol. Suppose that A has long-term secret key x with public key g^x and B has long-term secret key y with public key g^y. The protocol is then as follows.

   - A chooses random a and sends the value $A = g^a$ to B.
   - B chooses random b and sends the value $B = g^b$ to A.
   - A computes the session key $K_{AB} = B^x(g^y)^a$, using the received message Y and the long-term key of B.
   - B computes the session key $K_{BA} = A^y(g^x)^b$, using the received message X and the long-term key of A.

   (a) Show that A and B compute the same key: $K_{AB} = K_{BA}$.

   (b) Show that this protocol does not achieve the forward secrecy property.

5. Two signature schemes commonly used today are RSA signatures and DSA signatures. Suppose that the RSA modulus n has length 2048 bits and the DSA modulus p has length 2048 bits with length of parameter q equal to 224 bits. You may assume that the DSA parameters p and q are fixed for all parties.

   Alternate question: Parameters are $|n| = 3072$, $|p| = 3072$, $|q| = 256$.

   (a) RSA signatures often use a public exponent $e = 2^{16} + 1$. Approximately how much faster on average is signature verification with this value of e compared to when e is randomly chosen e?

   (b) What is the approximate ratio of the signature length, RSA against DSA?

   (c) What is the approximate ratio of the signing key length, RSA against DSA?

   (d) What is the approximate ratio of the verification key length, RSA against DSA?

6. Protection of metadata, typically included in header information in network protocols, is important in preserving privacy.

   (a) Compare what cryptographic protection is available for IP metadata in (i) IPSec in tunnel mode and (ii) TLS between a client and server.

   (b) Compare what cryptographic protection is available for email metadata in (i) PGP and (ii) STARTTLS.

   (c) Is there a conflict between protection of metadata and end-to-end security? Discuss such a conflict in the context of the above two examples.