University Djilali Bounaâma of Khemis-Miliana
Department of Mathematics and Computer Science
L3 – Computer Systems (S6)
Final Examination – IT Security & Cryptography
May 2024

Full Name - Group

……

Q1 (06 pts): Match each encryption/decryption formulas in the left with the appropriate block cipher mode in the right (C_i: Current Ciphertext block, P_i: Current Plaintext block), and indicate the parallelizability of each mode: (Matching: 04pts, Prallelizability: 0.25pt each)

	Encrypt/Decrypt Formulas	Block Cipher Mode	Encryption	Decryption
1	$C_i = E_k(C_{i-1}) \oplus P_i$ $P_i = E_k(C_{i-1}) \oplus C_i$	CBC	☐ Parallel ☒ Not-Parallel	☒ Parallel ☐ Not-Parallel
2	$C_i = P_i \oplus E_k(IV_{i-1})$ $P_i = C_i \oplus E_k(IV_{i-1})$	PCBC	☐ Parallel ☒ Not-Parallel	☐ Parallel ☒ Not-Parallel
3	$C_i = E_k(P_i) \oplus (P_{i-1} \oplus C_{i-1})$ $P_i = D_k(C_i) \oplus (P_{i-1} \oplus C_{i-1})$	OFB	☐ Parallel ☒ Not-Parallel	☐ Parallel ☒ Not-Parallel
4	$C_i = E_k(P_i \oplus C_{i-1})$ $P_i = D_k(C_i) \oplus C_{i-1}$	CFB	☐ Parallel ☒ Not-Parallel	☒ Parallel ☐ Not-Parallel

Q2 (02 pts): Match each description in the left with the corresponding type of attack in the right:

1. Collecting information, Recovering secret keys, Destroying channels		a. Dictionary attack
2. Determining repetitions of symbols in text, comparing them with typical occurrences of a language		b. Exhaustive search attack
3. Require as input the name of the file to decode and a regular expression to apply		c. Statistical attack
4. Deciphering a password by trying a set of words (reversed, lowercase, uppercase)		d. Protocol attack

Q3 (1.5 pts): Calculate the number of attempts of a brute force attack against a block cipher mode encryption (Block-size = 64 bits, Key = 64 bits) for the following cases:

1) Encrypt the same plaintext block two times using the same key and the same algorithm
   Number of attempts: 2^{64}
2) Encrypt the same plaintext block two times using the same algorithm with two different keys
   Number of attempts: 2^{128}
3) Encrypt the same plaintext block two times using two different algorithms and two different keys

Number of attempts: 2^{128}

Q4 (3.5 pts): List the steps that explain how a secured transaction goes between a Client and a Server owner of X509 certificate:

1) The client initializes the connection with the server
2) The server responds with the certificate
3) The client verifies the validity of the certificate by checking the verification authority database
4) The server sends its public key to the client
5) The server encrypts a secret key with its private key and send it to the client
6) The client decrypts the secret key using the public key of the server
7) The client and the server exchange secured transactions using the same secret key

Q5 (05 pts): List the steps to follow in order to create RSA public and private keys for someone (with examples):

1) Choose two coprime numbers p and q (0.5 pt)
   Example: p = 5, q = 17 (0.5 pt)
2) Calculate n = p × q

   Example: n = 5 × 17 = 85
3) Calculate φ(n) = (p-1) × (q-1)

   Example: φ(n) = 4 * 16 = 64
4) Find e coprime with φ(n): cgd(e, φ(n)) = 1
   Example: e = 5, cgd(5,64) = 1
5) Find d inverse of e modulo phi(n): e × d ≡ 1 (mod(φ(n)))

   Example: 5 × 13 = 1 (mod(64))

   Public key: e = 5, n = 85. Private key: d = 13

Q6 (02 pts): Use the data of the previous question (your examples) in order to sign a message of your choice, then verify its authenticity:

Example: M = 10

1) **Signature: (01 pt)**

$m_s = m^d$ (mod n) = 10^{13} (mod 85)

13 = 8+4+1

$10^{13} = 10^{8+4+1}$

$10^1 \equiv 10 \pmod{85}$

$10^2 \equiv 10 \times 10 \pmod{85} \equiv 100 \pmod{85} \equiv 15 \pmod{85}$

$10^4 \equiv 15 \times 15 \pmod{85} \equiv 225 \pmod{85} \equiv 55 \pmod{85}$

$10^8 \equiv 55 \times 55 \pmod{85} \equiv 3025 \pmod{85} \equiv 50 \pmod{85}$

$10^{13} \equiv 10^{8+4+1} \equiv 10^8 \times 10^4 \times 10 \equiv 50 \times 55 \times 10 \equiv 27500 \pmod{85} \equiv$ **45 (mod 85)**

2) **Authentication: (01 pt)**

$m = m_S^{\,e}$ (mod n) = 45^5 (mod 85)

5 = 4 + 1

$45^5 = 45^{4+1}$

$45^1 \equiv 45 \pmod{85}$

$45^2 \equiv 45 \times 45 \pmod{85} \equiv 2025 \pmod{85} \equiv 70 \pmod{85}$

$45^4 \equiv 70 \times 70 \pmod{85} \equiv 4900 \pmod{85} \equiv 55 \pmod{85}$

$45^5 \equiv 45^{4+1} \equiv 45^4 \times 45 \equiv 55 \times 45 \equiv 2475 \pmod{85} \equiv$ **10 (mod 85)**

The corrected version with a detailed grading scale will be published on the page http://cryptosdz.blogspot.com and on the elearning platform.