COMP 435: Extra Practice 4: Cryptography Name: _____

Practice through cryptographic hashes, MACs, and digital signatures. Show your work.

Question 1: RSA Practice For this small textbook RSA example, choose $p = 3$, $q = 5$, and $e = 3$. Use $c = m^e \bmod N$ and $m = c^d \bmod N$.

1.1. Compute N and $\varphi(N)$. Verify that e is relatively prime to $\varphi(N)$, then find d such that $ed \equiv 1 \pmod{\varphi(N)}$.

1.2. Encrypt $m = 2$, then decrypt the ciphertext. Show your arithmetic.

1.3. A professor uses textbook RSA to encrypt a grade from 0 to 100 with each student's public key and publishes the ciphertext. The modulus is much larger than 100. How can an observer recover the grade without the private key?

Question 2: Classical Ciphers and Attack Models 2.1. Could `MEET` encrypt to `ABCD` under a fixed one-to-one monoalphabetic substitution? Explain briefly.

2.2. Name each attack model: (i) observing only ciphertexts; (ii) obtaining existing plaintext–ciphertext pairs; (iii) choosing messages to have encrypted; (iv) choosing ciphertexts to have decrypted, excluding the target ciphertext.

2.3. Must a secure encryption algorithm remain secret? What should remain secret?

Question 3: One-Time Pads and Stream Ciphers Use XOR encryption, $C = M \oplus K$.

3.1. Encrypt $M = 1011$ with $K = 0110$, then recover M from your ciphertext.

3.2. State the requirements on a pad for an OTP to provide perfect secrecy. Does trying every pad identify the original message?

3.3. If a key stream is reused, simplify $C_1 \oplus C_2$. If Mallory knows M_1, what can she learn?

3.4. Mallory flips one ciphertext bit. What happens to the decrypted plaintext? Which security property is missing from XOR encryption alone?

Question 4: Block Cipher Modes 4.1. Two identical plaintext blocks are encrypted under one key in ECB mode. What relationship do their ciphertext blocks have? Why is this undesirable?

4.2. CBC encryption is $C_i = E_K(P_i \oplus C_{i-1})$, with $C_0 = IV$. Write its decryption equation. Can different blocks be decrypted in parallel once all ciphertext blocks are available?

4.3. In OFB and CTR, is block-cipher encryption or decryption used to generate the key stream when *decrypting*? What goes wrong if a key stream is reused?

Question 5: Diffie–Hellman Use public parameters $p = 11$, $g = 2$. Alice chooses secret $a = 3$ and Bob chooses secret $b = 4$. Use $A = g^a \bmod p$, $B = g^b \bmod p$, and $K = B^a \bmod p = A^b \bmod p$.

5.1. Find A, B, and K. Show that both parties get the same K.

5.2. In real DH with appropriately chosen large parameters, a passive observer sees p, g, A, and B. Is the shared secret transmitted? Does unauthenticated DH prevent an active attacker from impersonating the parties?

Question 6: Hybrid Encryption and Freshness Alice sends Bob an encrypted session key and an encrypted message: $\text{Enc}_{PK_B}(K)$ and $\text{Enc}_K(M)$.

6.1. Which key does Bob use to recover K? Why use a symmetric cipher for M?

6.2. Mallory records and later resends both ciphertexts unchanged. Does encryption alone let Bob recognize this as an old request? Describe how a fresh challenge could help.

Question 7: Cryptographic Hash Functions 7.1. Name the property targeted in each case: (i) finding any two different messages with the same hash; (ii) given one message, finding a different message with the same hash; (iii) given only a hash, finding a matching input.

7.2. Does collision resistance mean collisions do not exist? Explain.

7.3. For an ideal 128-bit hash, give the approximate powers of two for finding any collision and for finding a pre-image of a fixed hash.

7.4. A download and its hash are on the same compromised website. Can an attacker replace both without finding a hash collision?

Question 8: MACs and Digital Signatures Assume secure algorithms, uncompromised keys, and authentic public keys.

8.1. Alice and Bob share secret K. Alice sends $(M, \mathrm{MAC}_K(M))$. How does Bob verify it? Does this hide M? Could Bob create a valid tag himself?

8.2. Alice signs a software update. Which key creates the signature and which key verifies it? Why is a signature useful for public distribution?

8.3. Does a valid signature alone prove that a message is confidential or that it was sent recently? Explain briefly.

Solutions

1. RSA Practice

1.1 $N = 15$, $\varphi(N) = 8$, and $\gcd(3, 8) = 1$. $d = 3$ works because $3 \cdot 3 = 9 \equiv 1 \pmod 8$.

1.2 $c = 2^3 \bmod 15 = 8$. Decryption: $8^3 = 512 \equiv 2 \pmod{15}$.

1.3 Encrypt each of the 101 possible grades with the public key and compare against the ciphertext. Textbook RSA is deterministic. Secure randomized padding is needed; small classroom RSA examples are not secure deployments.

2. Classical Ciphers and Attack Models

2.1 No. The repeated E must map to the same ciphertext letter in both positions.

2.2 (i) Ciphertext-only; (ii) known-plaintext; (iii) chosen-plaintext; (iv) chosen-ciphertext.

2.3 No. Under Kerckhoffs' principle, security should depend on the secret key, not on secrecy of the algorithm.

3. One-Time Pads and Stream Ciphers

3.1 $C = 1101$; $1101 \oplus 0110 = 1011$.

3.2 The pad is uniformly random, independent of the message, secret, as long as the message, and never reused. Every same-length plaintext has a compatible pad, so exhaustive search alone cannot identify the original plaintext.

3.3 $C_1 \oplus C_2 = M_1 \oplus M_2$. She can recover $M_2 = C_1 \oplus C_2 \oplus M_1$.

3.4 The corresponding plaintext bit flips. Encryption alone provides no integrity/authentication check to detect the change.

4. Block Cipher Modes

4.1 They are identical, exposing repeated-block patterns in the plaintext.

4.2 $P_i = D_K(C_i) \oplus C_{i-1}$. Yes: each computation uses available ciphertext blocks, not the preceding plaintext result.

4.3 Encryption is used in both directions. Reuse reveals the XOR of the plaintexts, as in Question 3. OFB feedback is sequential; CTR counter blocks can be processed in parallel.

5. Diffie–Hellman

5.1 $A = 8$, $B = 16 \bmod 11 = 5$. Alice: $5^3 = 125 \equiv 4 \pmod{11}$. Bob: $8^2 \equiv 9$ and $8^4 \equiv 81 \equiv 4 \pmod{11}$.

5.2 K is not transmitted; each party derives it. Unauthenticated DH permits a man-in-the-middle to replace the exchanged public values and establish a separate secret with each party. The exchange must be authenticated.

6. Hybrid Encryption and Freshness

6.1 Bob's private key. Symmetric encryption is efficient for bulk data; public-key encryption protects the small session key.

6.2 No. Bob can issue a fresh nonce and require an authenticated response binding it to the request/session. He checks that it matches an outstanding, unused challenge and rejects reuse. A nonce alone, without checking and binding, is not enough.

7. Cryptographic Hash Functions

7.1 (i) Collision resistance; (ii) second pre-image resistance; (iii) pre-image resistance.

7.2 No. There are more possible messages than fixed-length hashes. Collisions exist, but finding one should be computationally infeasible.

7.3 Collision: 2^{64} hash evaluations; pre-image: 2^{128}. The birthday effect applies to any-pair collisions.

7.4 Yes. Replace the file and publish its newly computed hash. A hash comparison requires an authentic expected hash to establish integrity against this attacker.

8. MACs and Digital Signatures

8.1 Bob verifies the tag using K (typically recomputing it and comparing). M is sent in the clear. Bob also knows K and can create valid tags.

8.2 Alice's private signing key creates it; her public verification key checks it. Anyone with an authentic copy of that public key can verify without receiving a secret that would let them forge her signatures.

8.3 Neither. Signing does not encrypt the message, and an old signed message can be replayed. Freshness requires authenticated context and checks.