CPSC 418/MATH 318
MIDTERM EXAMINATION — ANSWERS

---

1. [10 marks] **Multiple Choice Questions**

   For each question, check exactly one answer.

   (a) Which of the following is *not* considered a service provided by cryptography?

   - ○ integrity
   - ○ access control
   - • usability
   - ○ they are all considered services provided by cryptography

   (b) The one-time pad is a

   - • monoalphabetic substitution cipher
   - ○ polyalphabetic substitution cipher
   - ○ transposition cipher
   - ○ product cipher

   (c) What is a product cipher?

   - ○ A cipher that uses byte multiplication in its encryption function
   - ○ A cipher in which encryption multiplies a plaintext by a key
   - ○ The application of one cipher, followed by the application of another necessarily different cipher
   - • The application of one cipher, followed by the application of another (identical or different) cipher

   (d) Under what necessary and sufficient condition is the entropy of a random variable maximal?

   - ○ No outcome has probability 0
   - ○ One outcome has probability 1 and all others have probability 0
   - • All outcomes are equally likely
   - ○ None of the above

   (e) Which of the following design elements achieves diffusion in a block cipher?

   - ○ Substitutions
   - • Permutations
   - ○ Hash functions
   - ○ One-way functions

(f) Consider a block cipher with m-bit keys. Then the number of bits of security provided by double encryption $C = E_{K_1}(E_{K_2}(M))$ is approximately

- m — due to the meet-in-the-middle attack
- $2m$
- m^2
- None of the above

(g) Consider a cryptosystem where m is the number of messages and k is the number of keys. If the system provides perfect secrecy, which of the following is true?

- $k < m$
- $k \geq m$
- $\gcd(k, m) = 1$
- we cannot say anything about the relationship between k and m

(h) [1 mark] Which of the following statements is true about a hash function f?

- If f is strongly collision resistant, then f is pre-image resistant
- If f is pre-image resistant, then f is weakly collision resistant
- If f is pre-image resistant, then f is strongly collision resistant
- None of the above

(i) Let p be a prime and $a \in \mathbb{Z}_p^*$ such that $a^{p-1} \equiv 1 \pmod{p}$. Which of the following can you conclude from these facts?

- a is a primitive root of p
- a is not a primitive root of p
- a is a prime
- None of the above — This is just Fermat's Little Theorem which holds for all $a \in \mathbb{Z}_p^*$

(j) Let $m, n \in \mathbb{N}$, and let ϕ denote Euler's phi function. Under what sufficient condition is $\phi(mn) = \phi(m)\phi(n)$?

- Only when m and n are relatively prime, i.e. $\gcd(m, n) = 1$
- Only when m and n are even
- Only when m and n are odd
- Always

2. [5 marks] **True/False Questions**

Circle the correct answer for each question. No explanations are required.

(a) [1 mark] Every block cipher can be converted to a stream cipher.

TRUE **FALSE**

(b) [1 mark] The MixColumns component of AES is a linear operation.

TRUE **FALSE**

(c) [1 mark] A known plaintext attack is an active attack.

TRUE **FALSE**

(d) [1 mark] The number of trials that need to be executed to find a pre-image of a pre-image resistant m-bit hash function is on the order of $2^{m/2}$.

TRUE **FALSE**

(e) [1 mark] Cryptographic hash functions are one-way functions.

TRUE **FALSE**

3. [19 marks] **Definitions and Short Answer Questions**

(a) [2 marks] Define a *chosen ciphertext attack* against a symmetric key cryptosystem.
Answer. Adversary chooses some ciphertext (independently of the ciphertext she wishes to decrypt) and obtains the corresponding plaintext.

(b) [2 marks] Describe how a transposition cipher acts on plaintexts to convert them to ciphertexts.
Answer. It permutes the plaintext characters/bits

(c) [2 marks] Let X and Y be random variables. State Bayes' Theorem.
Answer. $p(x|y) = \dfrac{p(x)p(y|x)}{p(y)}$ for all outcomes $x \in X, y \in Y$ with $p(y) > 0$.

(d) [2 marks] Let m be an integer with $m > 1$. Define the set $\mathbb{Z}_m^*$.
Answer. $\mathbb{Z}_m^* = \{a \in \mathbb{Z} \mid 0 \leq a \leq m-1, \gcd(a, m) = 1\}$.

(e) [2 marks] Describe the format of the state in the Keccak algorithm with width 1600.
Answer. A $5 \times 5 \times 64$ array of bits.

(f) [2 marks] Consider the shift cipher, where plaintexts, ciphertexts and keys are interpreted as integers modulo 26. Give the mathematical formula for the ciphertext C obtained by encrypting a shift cipher message M under a shift cipher key K.
Answer. $C \equiv M + K \pmod{26}$.

(g) [1 marks] How many bits of security does a 160-bit cryptographic hash function provide?
Answer. 80 bits (due to the birthday attack).

(h) [2 marks] Use the primitive root test to prove that 3 is a primitive root of 7. You must use the primitive root test; answers that do not use this test will receive no credit. Explain your work.
Answer. $7 - 1 = 2 \cdot 3$, so the prime factors of $7 - 1$ are 2 and 3.
$3^{(7-1)/2} \equiv 3^3 \equiv 27 \equiv 6 \not\equiv 1 \pmod{7}$.
$3^{(7-1)/3} \equiv 3^2 \equiv 9 \equiv 2 \not\equiv 1 \pmod{7}$.

(i) Let ϕ denote Euler's phi function.

i. [2 marks] State a formula for $\phi(p^3)$ when p is a prime.
Answer: $\phi(p^3) = p^3 - p^2 = p^2(p-1)$.

ii. [2 marks] Use your formula for $\phi(p^3)$ to compute $\phi(27)$.
Answer: $\phi(27) = \phi(3^3) = 3^2(3-1) = 18$.

4. [5 marks] **Probability and Entropy**

Consider a fair toss of two different coins, where each coin can come out 0 or 1. So the set of outcomes is $\{\,(0,0),\ (0,1),\ (1,0),\ (1,1)\,\}$, and each outcome has probability $1/4$.

Now consider the random variable X that models the sum of the outcomes of the two coins. Here, the set of outcomes is $\mathcal{X} = \{0,1,2\}$ because each sum consists of two terms that are 0 or 1.

(a) [3 marks] Compute the probability distribution on X. That is, compute the values $p(0), p(1), p(2)$.

Answer.

The sum 0 occurs only as $0 = 0 + 0$, i.e. if and only if both coins come out 0. So $p(0) = 1/4$.

The sum 1 can occur i two ways as $1 = 0 + 1 = 1 + 0$, i.e. when the one of the coins comes out 0 and the other comes out 1. So $p(1) = 1/2$.

Finally, the sum 2 occurs only as $2 = 1 + 1$, i.e. if and only if both coins come out 1. So $p(2) = 1/4$.

(b) [2 marks] Compute the entropy $H(X)$. Give you answer as a fraction or a decimal number.

Answer.

$$\begin{aligned} H(X) &= \frac{1}{4}\log_2(4) + \frac{1}{2}\log_2(2) + \frac{1}{4}\log_2(4) \\ &= \frac{1}{4}\cdot 2 + \frac{1}{2}\cdot 1 + \frac{1}{4}\cdot 2 = \frac{3}{2} = 1.5\ . \end{aligned}$$

5. [5 marks] **One-Time Pad**

Consider an online survey consisting of 20 questions with yes/no answers. Each survey participant encodes their answers as a 20-bit string where for $1 \leq i \leq 20$, the i^{th} bit is 1 is the answer to the i^{th} question is "yes" and 0 otherwise. The agency conducting the survey issues each participant a secret 20-bit one-time pad key, chosen randomly so each key is selected with equal likelyhood. Each participant uses their key to encrypt their answer strings with the one-time pad before submitting them online.

(a) [2 marks] Suppose Eve intercepts Alice's encrypted survey answer string. Without knowing the key issued to Alice by the agency, can Eve deduce on which of the questions Alice answered "yes"? Explain.

Answer: No. Let C_A be the Alice's encrypted answer string. Then for every string M_A of answers that Alice could have given, there exists a key K such that $C_A = M_A \oplus K$, namely $K = C_A \oplus M_A$. So C_A provides no information whatsoever about M_A.

Alternative explanation: the one-time pad provides perfect secrecy if every key is chosen equally likely. So for every string M_A of potential answers that Alice could have given, $p(M_A|C_A) = p(M_A)$. In other words, knowing C_A does not increase the likelihood of any string M_A, compared to not knowing C_A.

(b) [3 marks] Suppose now that Eve intercepts Alice's and Bob's encrypted survey answer strings. Suppose also that Eve knows that the surveying agency has (carelessly!) issued Alice and Bob the same key to encrypt their answers, but Eve does not know this key. Can Eve deduce on which of the questions Alice and Bob gave the same answer? Explain.

Answer: Yes. Let M_A and M_B be Alice's and Bob's respective answer strings, and let $C_A = M_A \oplus K$ and $C_B = M_B \oplus K$ be their respective encryptions under the key K used by both Alice and Bob. Then identical answers correspond exactly to identical bits in the same positions in M_A and M_B, which in turn correspond exactly to identical bits in C_A and C_B because M_A and M_B were X-OR'ed with the same key. So Alice and Bob gave the same answers exactly on those questions that correspond to positions in C_A and C_B with identical bits.

Another way of stating this is to note that $C_A \oplus C_B = M_A \oplus M_B$, so the zero bits in $C_A \oplus C_B$ correspond precisely to the questions where Alice and Bob gave the same answer.

Common errors: Quite a few people asserted that $C_A \oplus C_B = K$ which is absolutly not true! Others claimed that Even can find the key in some other way, including via exhaustive search. This is also not true. In particular, the whole point of perfect secrecy is that it is impossible to brute-force keys beause you cannot distinguish the correct decryption from any other plaintext.

6. [5 marks] **Polynomial Arithmetic**

Let

$$f(x) = x^4 + x^3 + 1$$
$$g(x) = x^2 + x$$

be polynomials with binary coefficients. Compute

$$f(x)g(x) \pmod{x^5 + x^4 + 1} .$$

Answer: $f(x)g(x) = (x^4 + x^3 + 1)(x^2 + x) = x^6 + x^5 + x^2 + x^5 + x^4 + x = x^6 + x^4 + x^2 + x$ in binary coefficient arithmetic. Modulo $x^5 + x^4 + 1$, we have

$$x^5 = x^4 + 1 ,$$
$$x^6 = x \cdot x^5 = x(x^4 + 1) = x^5 + x = (x^4 + 1) + x = x^4 + x + 1 ,$$

It follows that

$$f(x)g(x) = (x^4 + x + 1) + x^4 + x^2 + x \equiv (x^4 + x^2 + x + 1) + x \equiv x^2 + 1 \pmod{x^5 + x^4 + 1} .$$

7. [6 marks] **Diffie-Hellman**

Let p be a prime and g a primitive root of p.

(a) [2 marks] State the discrete logarithm problem. Be sure to define all your notation (except for p and g which were already defined above).

Answer: Given p, g and $g^x \pmod p$ with $0 \leq x \leq p-2$, find x.

(b) [2 marks] State the Diffie-Hellman problem. Be sure to define all your notation (except for p and g which were already defined above).

Answer: Given p, g and $g^a \pmod p$ and $g^b \pmod p$ with $0 \leq a, b \leq p-2$, find $g^{ab} \pmod p$.

(c) [2 marks] Suppose you have an algorithm for efficient extraction of discrete logarithms. Carefully and succinctly explain how you can use this algorithm to solve any instance of the Diffie-Hellman problem.

Answer: Le $(p, g, g^a \pmod p, g^b \pmod p))$ be an input to the Diffie-=Helmman problem. The adversay uses the discrete logarithm algorithm on input $(p, g, g^a \pmod p))$ to obtain a. Then she computes $(g^b)^a \equiv g^{ab} \pmod p$.

Alternatively, she could also use her DLP algorithm on input $(p, g, g^b \pmod p))$ to obtain b. Then she computes $(g^a)^b \equiv g^{ab} \pmod p$.

A third alternative is to compute both a and b, then ab, then $g^{ab} \pmod p$.

8. [5 marks] **Hash Functions and Message Authentication Codes**

(a) [2 marks] Define what it means for a message authentication code to be *computation resistant*.

Answer: For any key K, given zero or more message/MAC pairs $(M_i, MAC_K(M_i))$, it is computationally infeasible to compute, without knowledge of K, any new message/MAC pair $(M, MAC_K(M))$ with $M \neq M_i$ for all i.

(b) [3 marks] Let $h : \{0,1\}^* \to \{0,1\}^n$ be an n-bit pre-image resistant hash function ($n \in \mathbb{N}$). Define a message authentication code, derived from h, that operates on n-bit messages via

$$MAC_K(M) = M \oplus h(K)$$

for any $M \in \{0,1\}^n$. Formally prove that this message authentication code is not computation-resistant.

Answer: There are many solutions to this question; I'll give four which were all found by students in the class. We have $MAC_K(M) = M \oplus h(K)$, so Eve can compute

$$h(K) = MAC_K(M) \oplus M \ .$$

Eve now generates any $M' \in \{0,1\}^n$ with $M' \neq M$ and computes

$$MAC_K(M') = M' \oplus h(K)$$

without knowledge of K.

Another solution is for Eve to choose $M' = 0^n$. Then $MAC_K(M') = 0^n \oplus h(K) = h(K)$ (which she computes as before), so $(0^m, h(K))$ is a valid message/MAC pair.

Some students came up with other approaches. For example, a solution that does not require explicitly computing $h(K)$, is to use two different intercepted message/MAC pairs $(M_1, MAC_K(M_1))$ and $(M_2, MAC_K(M_2))$ and choose $M_3 = M_1 \oplus M_2$. Then

$$M_1 \oplus MAC_K(M_1) = M_1 \oplus M_2 \oplus h(K) = MAC_K(M_1 \oplus M_2),$$

so $(M_1 \oplus M_2, M_1 \oplus MAC_K(M_1))$ is a valid message/MAC pair, as long as neither M_1 nor M_2 is 0^n (so M_3 is different from both M_1 and M_2).

You could even work with three different intercepted message/MAC pairs $(M_i, MAC_K(M_i))$ for $i = 1, 2, 3$ and choose $M_4 = M_1 \oplus M_2 \oplus M_3$, which is different from M_1, M_2, M_3 because these three are all different (conbince yourself of this). Then

$$\begin{aligned} &MAC_K(M_1) \oplus MAC_K(M_2) \oplus MAC_K(M_3) \\ &\qquad = (M_1 \oplus h(K)) \oplus (M_2 \oplus h(K)) \oplus (M_3 \oplus h(K)) \\ &\qquad = M_1 \oplus M_2 \oplus M_3 \oplus h(K) = M_4 \oplus h(K) = MAC_K(M_4) \ . \end{aligned}$$

So if Eve computes $h(K)$ as before, she has found a valid message$(M_4, MAC_K(M_4)) = (M_1 \oplus M_2 \oplus M_3, MAC_K(M_1) \oplus MAC_K(M_2) \oplus MAC_K(M_3)$.

Common error: Some students wanted to come up with a string K such that $h(K) = 0^n$, in which case the MAC of any message M' is the same as the message M' itself. But that would require finding a pre-image under h, contradicting the assumption that h is pre-image resistant.