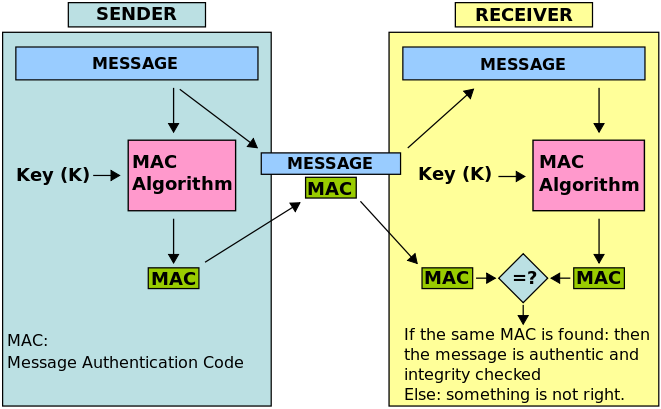
**Problem 1 (10 points).**

**(a) What is message integrity, and how does a MAC (message authentication code) ensure it?**

**(b) Draw a diagram that illustrates the way a MAC interacts with a message between Alice and Bob in CBC (cipher block chaining) mode.**

Message integrity is verification that the message sent has not been tampered with. This is ensured with a Message Authentication code. The message authentication code is a key(symmetric) dependent one way hash function. The message is encrypted with the MAC algorithm and sent along with the message. The receiver also runs the message through the same MAC algorithm with the key and if the output is the same, the receiver can assume the message is genuine. To protect against replay attacks, the payload must contain some unique information such as a time stamp so the message cannot be resent.



**Problem 2 (5 points).**

**What is the GCD of 9774 and 234? Show all work using Euclid’s Algorithm. Specifically, show the status after each iteration – you do not need to show computation of remainders.**

9774 = 234(41) + 180

234 = 180(1) +54

180 = 54(3) + 18

54 = 18(3) + 0

**Problem 3 (5 points).**

**Consider the private-key ciphers we studied in class (substitution cipher, shift cipher, Vigenere’s cipher). Define a chosen-plaintext attack, and explain why the aforementioned ciphers are vulnerable in this attack model. Is the one-time pad vulnerable in this model? The two-time pad (i.e., the one-time pad with a re-used pad)? Why or why not?**

A chosen-plaintext attack is an attack model where the attacker can choose a batch of chosen plaintext message, send them to the encryption oracle(black box) and receive corresponding cipher text for each plaintext. The substitution cipher, shift cipher, and vigeneres cipher are all susceptible to a chose plaintext because they are weak ciphers and a lot of information is revealed for the cryptanalyst in a chosen plaintext attack. For the shift cipher, the shift key can easily be discovered by a chose plaintext attack. For the simple substitution cipher, although the key space is larger than the shift cipher, a mapping could trivially be discovered by a chosen plaintext attack. Finally, for the Vigeneres cipher this attack still works but is not as easy. The length of the key could be discovered, then a frequency analysis could be done to solve for the key. Additionally, all three of these ciphers are vulnerable to cipher-text only attack, a weaker threat model so naturally they would be vulnerable to a chosen plaintext attack. The one-time pad isn’t vulnerable to any threat model because it is proved to have perfect secrecy. The two-time pad would be susceptible because it would significantly weaken the encryption by reusing the key/pad, to a method called crib dragging.

**Problem 4 (10 points).**

**Prove that 38209001 is not a prime using Fermat’s Little Theorem. (Hint: Proceed by contradiction. Assume to the contrary that 38209001 is a prime, and show that this contradicts Fermat’s Little Theorem. You may use Wolfram Alpha to compute modular powers.)**

Assume 38209001 is prime. That would mean that ap-1 = 1 mod p. So we can substitute in an integer for a, say 4. So if p is prime then 4p-1 = 1 mod p. So plugging in the numbers to wolfram we get a result of 24542863 mod 38209001 which does not equal 1 mod p, therefore 38209001 is not prime!

**Problem 5 (10 points).**

**(a) Does the set {1, 3} form a group under multiplication modulo 5? Why or why not?**

No because 3-1 is not in the set, which would be in this case 2. The set does not contain the multiplicative inverse of 3.

**(b) Does the set {1, 6} form a group under multiplication modulo 7? Why or why not?**

Yes because all three properties are satisfied. The identity is present, the multiplicative inverse’s are present, and any element multiplied with any element mod 7 exists in the set.

**Problem 6.**

**Answer the following. Fill in the blanks where provided.**

**(a) (1 point). What is the identity element in the additive group Zn?**

**(b) (1 point). What is the identity element in the multiplicative group Zp\* ?**

**(c) (2 points). What is the additive inverse of 18 modulo 29? Hint: your answer must be an integer between 0 and 28.**

**(d) (6 points). What is the multiplicative inverse of 19 in Z ∗ 23? (Show work below.)**

a. 0 b. 1 c. 11

d.

23 = 19(1) + 4

19 = 4(4) +3

4 = 3(1) + 1

3 = 1(3) + 0

1 = 4 – 3(1)

= 4 –19 + 4(4) = 4(5) -19

= (23 – 19)(5) – 19 = 23(5) + 19(-6)

-6 mod 23 = **17**

**Problem 7 (10 points).**

**(a) Encrypt the following phrase using the Vigenere cipher with the keyword COFFEE: COLDBREWPLEASE**

**(b) The Vigenere keyword is CWM and the cipher text is PWFWNMNHK. What is the message?**

COFFEECOFFEECOF

COLDBREWPLEASE

**ECQIFVGKUQIEUS**

CWMCWMCWM

PWFWNMNHK

**NATURALLY**

**Problem 8 (10 points). We wish to find the multiplicative inverse of 18 in Z ∗ 1491823. Let’s follow the following steps:**

**(a) Use Euclid’s Extended Algorithm to find r and s such that r · 18 + s · 1491823 = 1 Show your work. In other words, show the status of the algorithm after each step.**

**(b) How can you use part (a) to deduce the multiplicative inverse of 18 modulo 1491823?**

1491823 = 18(82879) + 1

18 = 1(18) + 0

1 = 1491823 + 18(-82879)

= 0 + 18(-82879)

-82879 mod 1491823 = **1408944**

**=** 18(**1408944) =** 1 mod1491823

**Problem 9 (5 points). What is a length extension attack against a MAC and what are ways we could defend against it?**

A length extension attack is a vulnerability of the Merkle-Damgard based hashes. It is when an attacker chains on M’ to the output of the hash(H(M1)) which includes the secret + payload. The result is an extended message with the attackers extended message which verifies to the receiver because it includes the senders original secret, without the attacker needing to know it. Ways to defend against this attack is to not use Merkle-Damgard bashed hashes and use HMAC.

**Problem 10 (5 points). Suppose you have a 50-bit string that contains exactly 37 ones at random positions. How many bits of entropy does this string contain? Show all work.**

= 226.59 = 26.59 bits of entropy