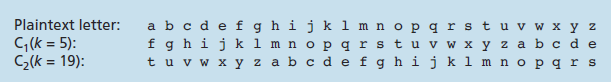
Cybersecurity Cryptography Homework

1. From a service perspective, what is an important difference between a symmetric-key system and a public-key system?
2. Can you “decrypt” a hash of a message to get the original message? Explain your answer
3. Consider a variation of the MAC algorithm where the sender sends (*m*, *H*(*m*) *+ s*), where m is the message and *H*(*m*) + *s* is the concatenation of *H*(*m*) and *s*, which is the secret key. Is this variation flawed? Why or why not?
4. Suppose certifier.com creates a certificate for foo.com. Typically, the entire certificate would be encrypted with certifier.com’s public key. True or False?
5. In the SSL record, there is a field for SSL sequence numbers. True or False?
6. Consider the polyalphabetic system shown below. Will a chosenplaintext attack that is able to get the plaintext encoding of the message “The quick brown fox jumps over the lazy dog.” be sufficient to decode all messages? Why or why not



1. What is the difference and similarity of MAC and a digital signature?
2. Provide a detailed diagram of how the CA public key and the server’s public key are used in SSL.
3. Extending the last question, list all the steps from the company that owns the server getting the public key certificate to the client getting the public key from the server. Now, list two possible security vulnerability and indicate how likely the vulnerability could be exploited.
4. In SSL, why is symmetric key encryption used when public key encryption is also used. Could public keys be used without symmetric key? If so, why is symmetric used.
5. Use the certificate explorer in chrome to view an SSL certification. Generate screen shots that show the certificate path and the expiration date. Find examples where the Subject field shows that only specific URLs are signed (like www.example.com) and an example when an entire domain is signed (like \*.example.com)
6. Installing fake certificate authority public keys (see https://udel.instructure.com/courses/1498333/files/84167431/download)
   1. Suppose a hacker installs a new certificate authority public key on a computer, what will that allow?
   2. Now suppose that a company installs their own certificate authority public key on an employee laptop. Why would a company install its own certificate authority public key on employee machines?
   3. What are the security threats of a company installing a CA public key on employee laptops?
7. Covid-19 contact tracing:
   1. Option 1. Each phone broadcasts the phone’s phone number. All nearby phones receive those numbers and the time when the number was received. If someone gets sick, all saves phone number are call. Why is this a privacy risk
   2. Option 2. Each phone has the health department’s public key and broadcast’s its phone number encrypted via the health department’s public key. Each phone records the encrypted phone numbers of the nearby phones and the time when received.
      1. What happens when someone is found to be sick?
      2. Does this option solve the privacy issues that the first option suffers from?
      3. Are there other privacy issues?
      4. Should a nonce be used to improve privacy?
8. My browser sometimes shows the text https crossed out and an “x” on a lock symbol. What does this mean? Is there a security risk? If so, explain how the vulnerability could be exploited.

