COSC130 Fundamentals of Cybersecurity and Privacy

Tutorial Week 9 Solutions

1. Using 6 columns, the plaintext SYDNEY OLIMPIC GAMES is written by rows as

S	Y	D	N	E	Y
O	L	Y	M	P	I
C	G	A	M	E	S

If the columns are taken off in the order 6-5-2-4-1-3 the resulting ciphertext is YISEPEYLGNMMSOCDYA.

What is the enciphering algorithm, and what is the key?

Solution:

The algorithm: plaintext is written into a matrix by rows and the ciphertext is obtained by taking off the columns in some order.

The key: There are 6 columns, and the order in which the columns are taken is 6-5-2-4-1-3, so the key is (6, 6-5-2-4-1-3); it would also be correct to say that the key is just the permutation 6-5-2-4-1-3, as the number of columns is clear from the permutation.

2. Suppose that we divide the plaintext SYDNEY OLYMPIC GAMES (blanks should be ignored) into blocks of 6 letters each, and we permute each block according to the following permutation: 6-5-4-3-2-1. What is
   1) the ciphertext
   2) the cipher
   3) the key?

Solution:

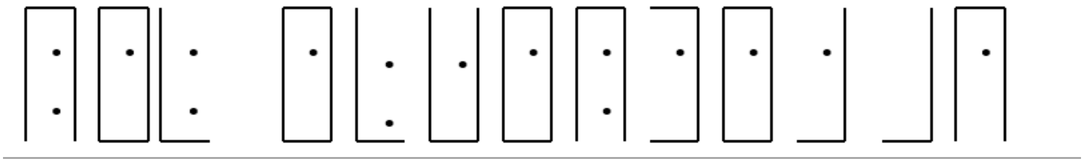
When we divide the plaintext into blocks of 6 letters, we get the following blocks: SYDNEY-OLYMPI-CGAMES.

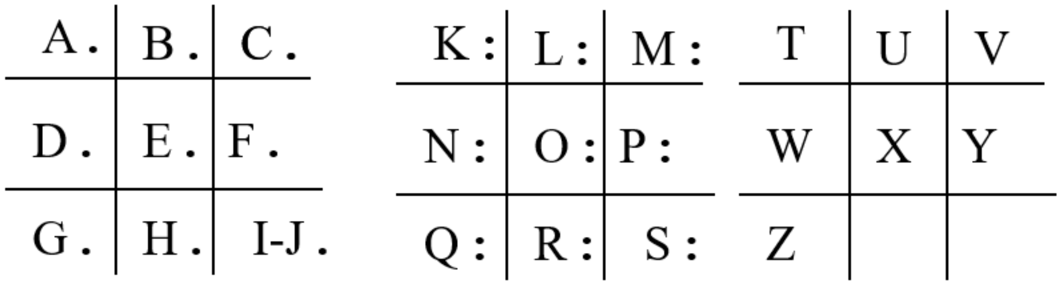
a) The ciphertext is YENDYS-IPMYLO-SEMAGC.

b) The cipher is to divide the plain text into blocks of size *s*, and to permute each block according to a given permutation.

c) The key is the blocks size *s*, and the permutation.

3. Using the key provided, decrypt the following cyphertext engraved on a tombstone in Trinity Churchyard, New York, 1794:





Solution:

REMEMBER DEATH

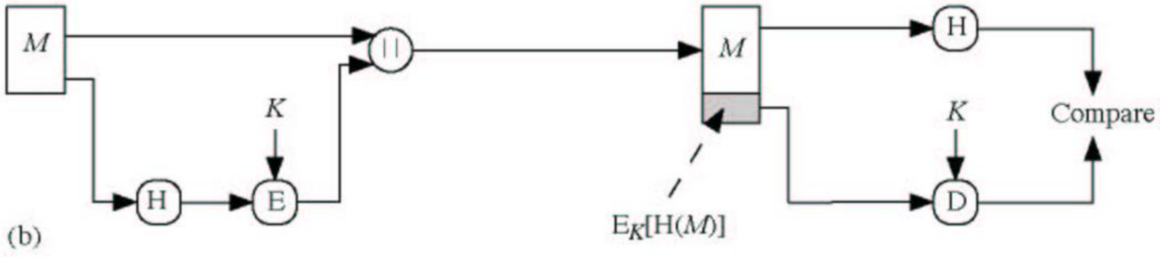
4. Consider the following three ways to authenticate messages: Encryption, Message Authentication Code (MAC), and hash function. For each of the following properties, specify which authentication method(s) they refer to:

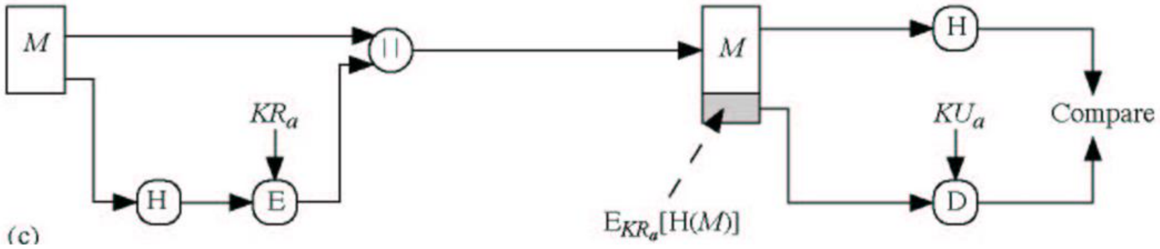
    1) Can be applied to a block of data of any size
    2) Produces a variable-length output
    3) Must be reversible

Solution:

a. All three methods must be able to be applied to a block of data of any size.
b. Only encryption produces a variable-length output.
c. Only encryption must be reversible.

5. In regards to digital signature, we typically do not sign the whole message; instead we first obtain a hash code of the message and then sign the hash code. Which one of the following two methods provide the digital signature and why?





Note that KR_a denotes for the private key of user "a", while KU_a denotes the public key of user "a".

Solution:

The second picture, labelled with (c), depicts a digital signature as the user "a" signs the hash code with their private key – nobody else can do it.

In picture (b), symmetric encryption with a single key is used, so both the sender and the recipient could have encrypted the hash code of the message. Therefore, picture labelled with (b) provides authentication, but does not provide a digital signature.

6. Represent the Diffie-Helmann key exchange protocol in 6 steps, assuming that the two participants have already exchanged the global elements.

   Solution:

   1) User A selects their private key X_A and computes their public key Y_A.
   2) User B selects their private key X_B and computes their public key Y_B.
   3) User A sends their public key Y_A to user B.
   4) User B sends their public key Y_B to user A.
   5) User A computes the secret key K.
   6) User B computes the secret key K.

7. Consider two nodes that are connected through a single 100Mbps (100 Megabits per second) network connection to the Internet. Imagine that one of these nodes wishes to send a 1GB (Gigabyte) message across the network.

1) How long would it tie up the line, preventing the other node from communicating, to send the 1GB message in one go, rather than first breaking it up into independent packets?

   Solution:

   1GB = 1024 MB = 1024 * 1024 KB = 1024 * 1024 * 1024 bytes = 8 * 1024 * 1024 * 1024 bits = 8,589,934,592 bits

   100 Mbps = 100,000,000 bits per second

   8,589,934,592 bits / 100,000,000 bits per second = 85.89… seconds

   The line would be held up for nearly 1.5 minutes

2) How long would it tie up the line, preventing the other node from communicating, to send a 1,500-byte packet, after the 1GB message was broken up into packets of this size?

   Solution:
   1,500 bytes = 1500*8 bits = 12,000 bits
   100 Mbps = 100,000,000 bits per second
   12,000 bits / 100,000,000 bits per second = 0.00012 seconds
   The line would be held up for 0.00012 seconds, after which time the other node may send a packet of its own (if it didn't want to, the original node could send the next packet in its message).

8. Imagine that Alice is sending a message to her bank to transfer $1,000, and that this message is encrypted using symmetric encryption. If Bob attempts to intercept this message and change the amount to $1,000,000, what will happen?

   Solution:
   Assuming a reasonable symmetric cypher and key were being used, Bob would not be able to read the message to see where to change it. If he did change it anyway, when the bank decrypted the message, the decrypted message would probably not be correctly formatted, and the bank would let Alice know an error had occurred.

9. Imagine a small e-commerce website that operates on a shared hosting server. This server typically handles a moderate amount of traffic from customers. Outline the potential impact of a DDoS attack on the e-commerce website in terms of website performance, availability, and customer experience.

   Solution:
   The volume of traffic would slowly bring the website to a crawl, until eventually resources such as CPU, memory, or network bandwidth were exhausted. This would cause website downtime, meaning legitimate customers would be unable to access the website. This could lead to a loss of revenue because potential

customers may get frustrated and abandon their sessions (perhaps to go to a competitor). Customers may also lose trust in the site, making them unlikely to return in the long term.

10. Imagine you are working in a coffee shop and need to access sensitive company data over the public Wi-Fi network. How would a Virtual Private Network (VPN) secure your connection? Are there any drawbacks from using a VPN?

    Solution:
    A VPN establishes a secure, encrypted connection over the Internet. It serves as a protective tunnel for Internet traffic, ensuring data remains confidential and secure while travelling across the public network.
    The main drawbacks would be slower Internet speed, since all requests are going through a remote server, and reduced battery life, since encryption does require additional computation.