COSC130 Fundamentals of Cybersecurity and Privacy

Tutorial Week 9

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

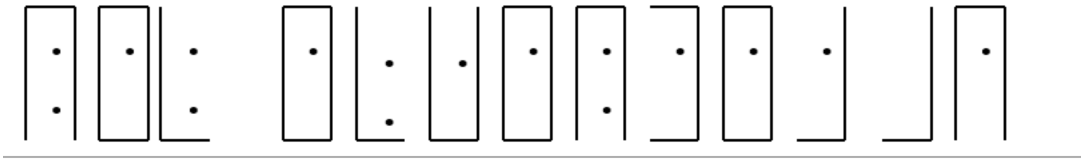
S	Y	D	N	E	Y
O	L	Y	M	P	I
C	G	A	M	E	S

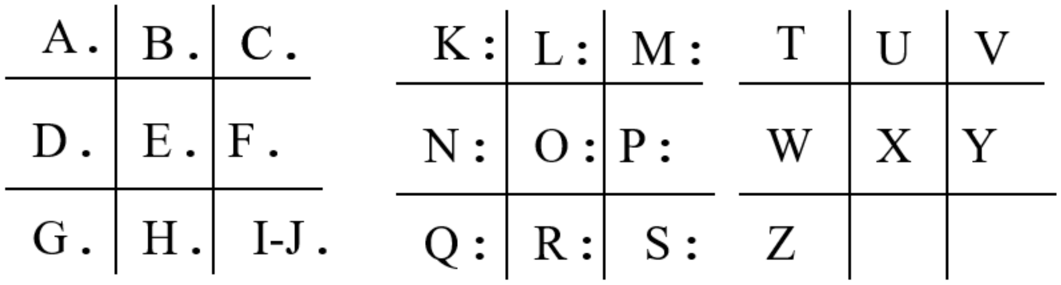
   If the columns are taken off in the order 6-5-2-4-1-3 the resulting ciphertext is YISEPEYLGNMMSOCDYA.

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

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?

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





A .	B .	C .
D .	E .	F .
G .	H .	I-J .

K :	L :	M :
N :	O :	P :
Q :	R :	S :

T	U	V
W	X	Y
Z		

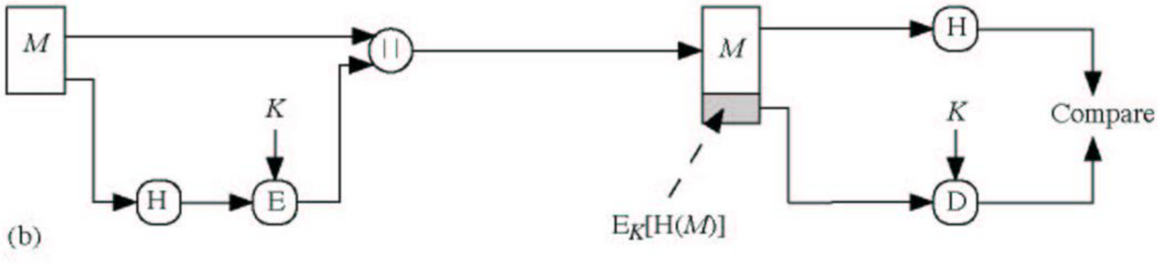
4. Consider the following three ways to authenticate messages: Encryption, Message Authentication Code (MAC), and hash function. For each of the following properties, specify which authentication method(s) they refer to:

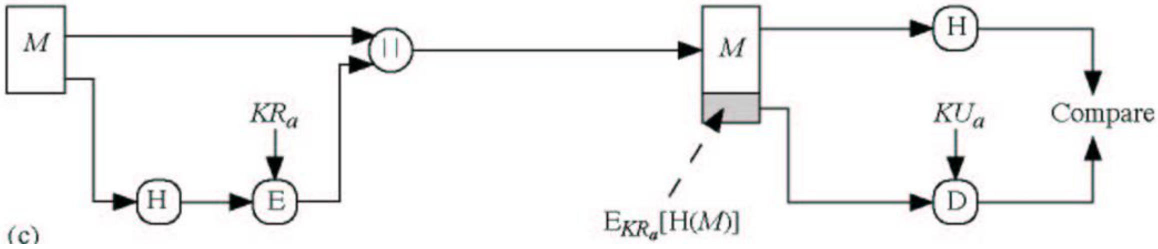
    1) Can be applied to a block of data of any size

    2) Produces a variable-length output

    3) Must be reversible

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".

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

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?

    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?

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?

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.

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?

.