CS5285: Information Security for eCommerce Autumn, 2024
Tutorial 2

1. **Caesar Cipher**: Julius Caesar was said to have used a shift cipher to encrypt messages. Assume that he sent the message below, can you recover the plaintext?
   Hint: The two most frequent characters in the plaintext of the ciphertext below are "E" and "I".

   `LFDPHLVDZLFRQTXHUHG`

2. **Substitution Cipher**

   (a) Using the substitution alphabet given below, what is the ciphertext of the plaintext phrase `ecommerce`?

a	b	c	d	e	f	g	h	i	j	k	l	m
R	O	F	D	E	U	Q	I	T	A	H	V	L
n	o	p	q	r	s	t	u	v	w	x	y	z
B	Y	W	N	S	J	P	M	X	C	G	K	Z

   (b) Using the same substitution alphabet, what is the plaintext of the ciphertext `JKLLEPSTF`?

3. **One-Time Pad**:

   (a) Alice wants to send the message `HELLO` to Bob using a one-time pad with the key `ABCDE`. What is the ciphertext?

A	B	C	D	E	F	G	H
0000	0001	0010	0011	0100	0101	0110	0111
I	J	K	L	M	N	O	P
1000	1001	1010	1011	1100	1101	1110	1111

   (b) What is the plaintext you get if you decrypt the ciphertext from 3(a) with the key `FOBEL`?

   (c) Give one disadvantage of one-time pad encryption.

4. **Stream Cipher**:

   (a) During an e-banking transfer the bank uses a stream cipher to encrypt data between the client and the bank's server. The client is required to enter the target account, amount and one-time password (using a device that generates him/her a password for each transaction) in a web form. This form data is encrypted, uploaded and if the password is correct the transaction is made. An attacker knows the format of the form (i.e. type of data being sent, length of fields) and he knows that each month on the same date you pay your rent to an agent. The attacker also rents from this agent so he knows the bank account number. If the attacker gets hold of the message can he make some money?

   (b) What additional security service do we need if we are using stream ciphers?