CSS322 – Quiz 1 Answers

Name: ______________________________

ID: ____________________ Mark: __________ (out of 10)

For reference, you may use the following mapping of English characters to numbers:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Question 1 [2.5 marks]

The Thai alphabet has 76 characters (ignoring special characters and punctuation). Assume a modified Caesar cipher was created to operate on the Thai alphabet.

a) Write an equation the describes the encryption/decryption operation of the Thai-based Caesar cipher, assuming a plaintext character *p*, key *k* and ciphertext character *c*. [1.5 marks]

Answer

Similar to the English-based Caesar cipher covered in the lectures, to encrypt take the input plaintext character and shift by key. However with 76 characters to "wrap around" we should mod by 76.

$$c = (p + k) \bmod (76)$$

To decrypt:

$$p = (c - k) \bmod 76$$

b) How many possible keys are there for the Thai-based Caesar cipher? [1 mark]

Answer

The key can be any of the characters, hence 76 possible keys.

Question 2 [2.5 marks]

Encrypt the first 8 characters of your name using a Vigenere cipher and the key SIIT. Start with your first name, and if it is less than 8 characters continue with your second name, ignore spaces (for example, I would encrypt: "stevengo"). Write your final answer here:

___ ___ ___ ___ ___ ___ ___ ___

Answer

Using “stevengo” as the input plaintext and with key “siit”:

Plaintext		Key		Ciphertext		
s	18	s	18	36	10	k
t	19	i	8	27	1	b
e	4	i	8	12	12	m
v	21	t	19	40	14	o
e	4	s	18	22	22	w
n	13	i	8	21	21	v
g	6	i	8	14	14	o
o	14	t	19	33	7	h

Hence the ciphertext is “kbmowvoh”.

Question 3 [3 marks]

Consider a system with two normal users Apiwat and Benjarak, and a malicious user Chinorot. The following statements describe *either* a security service required by the normal users *or* an attack performed by the malicious user. If the statement describes a service, then give the name of the service. If the statement describes an attack, give the name of the attack.

a) Benjarak wants to be certain that the message came from Apiwat, and not from Chinorot.

Service *or* attack: ___________________________

b) Chinorot obtains a copy of a message sent from Apiwat to Benjarak, and Chinorot tell's his friends about the message contents.

Service *or* attack: ___________________________

c) Chinorot sends many messages to Benjarak so that her computer is too busy to receive messages from Apiwat.

Service *or* attack: ___________________________

d) Benjarak wants to be certain that Chinorot has not changed the original message sent by Apiwat.

Service *or* attack: ___________________________

e) Chinorot notices messages being sent by Apiwat to Benjarak, and makes observations about how Apiwat and Benjarak are communicating.

Service *or* attack: ___________________________

f) Chinorot intercepts a message sent from Apiwat to Benjarak, and changes the message before sending on to Benjarak.

Service *or* attack: ___________________________

Answers

a. Authentication service; b. Release message contents attack; c. Denial of service attack; d. Data integrity service; e. Traffic analysis attack; f. Modification attack.

Question 4 [2 marks]

Assume I designed my own cipher to encrypt exam answers. The cipher uses a 40/50 bit key. I always create the answers 10 days before the exam and store them on my office computer, however on the same day that I created the exam answers a malicious student obtained access to my office computer and took a copy of the answers. The malicious student has free access to a computer that can decrypt the answers at a rate of 200×10^9 attempts per day (as the student wants to cheat on the exam, they don't know about any limitations in the encryption algorithm). Is this system used for encrypting exams computationally secure? Explain your answer, showing any calculations where necessary.

(Note that $2^{10} \approx 10^3$, $2^{20} \approx 10^6$, $2^{30} \approx 10^9$, and so on)

Answer

If the student applies a brute force attack, the maximum time to find an answer is:

40 bit key: $\approx 10^{12}$ combinations, at a rate of 2×10^{11} per day would take 5 days to find the answers. On average it would be even less. Therefore with this key size the system is not computationally secure because the malicious student could obtain valuable information will that information is still valid (i.e. before the exam).

50 bit key: $\approx 10^{18}$ combinations, at a rate of 2×10^{11} per day would take more than 5000 days to find the answers. On average less than half that (e.g. 2500 days) but still the malicious student cannot find the answers before the exam. Therefore it is considered computationally secure, because the time to find the answers is much greater than the valid lifetime of the information.

(Of course this may change if the conditions change, e.g. the student has access to a much faster computer or supercomputer).