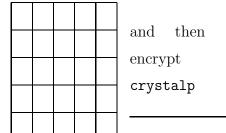
CMPUT 210 quiz 1 60 min closedbook 42 marks page 1

- 1. [2] Vigenere cipher, keyword stew, encrypt fleenow \_\_\_\_\_
- 2. [2] Kama Sutra cipher, key ab cd ef gh ij kl mn op qr st uv wx yz, encrypt fleenow \_\_\_\_\_\_
- 3. [2] scytale cipher, circumference 4, encrypt fleenow \_\_\_\_\_
- 4. [2] book cipher, key The vast sun was past its zenith, hot like an xray. Giant pandas raced back and forth. A mangy cat jumped on the kid, until then quietly eying the dozing newt. He yelped. encrypt fleenow
- 5. [4] Playfair cipher, keyword charlay, show the encryption Polybius grid



ABCDEFGHIJKLMNOPQRSTUVWXYZ 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 A C D E F G H I J K L M N O P Q R S T U V W X Y Z A B D E F G H I J K L M N O P Q R S T U V W X Y Z A B C E F G H I J K L M N O P Q R S T U V W X Y Z A B C D F G H I J K L M N O P Q R S T U V W X Y Z A B C D E G H I J K L M N O P Q R S T U V W X Y Z A B C D E F HIJKLMNOPQRSTUVWXYZABCDEFG IJKLMNOPQRSTUVWXYZABCDEFGH J K L M N O P Q R S T U V W X Y Z A B C D E F G H I K L M N O P Q R S T U V W X Y Z A B C D E F G H I J LMNOPQRSTUVWXYZABCDEFGHIJK M N O P Q R S T U V W X Y Z A B C D E F G H I J K L NOPQRSTUVWXYZABCDEFGHIJKLM O P Q R S T U V W X Y Z A B C D E F G H I J K L M N PQRSTUVWXYZABCDEFGHIJKLMNO QRSTUVWXYZABCDEFGHIJKLMNOP RSTUVWXYZABCDEFGHIJKLMNOPQ STUVWXYZABCDEFGHIJKLMNOPQR TUVWXYZABCDEFGHIJKLMNOPQRS UVWXYZABCDEFGHIJKLMNOPQRST V W X Y Z A B C D E F G H I J K L M N O P Q R S T U WXYZABCDEFGHIJKLMNOPQRSTUV X Y Z A B C D E F G H I J K L M N O P Q R S T U V W YZABCDEFGHIJKLMNOPQRSTUVWX ZABCDEFGHIJKLMNOPQRSTUVWXY

6. [2] ADFGVX ciphertext after first stage of encryption: DV DD DD DV FG FD DV DD AV XG AD GX.

The keyword is WETS. Give the ciphertext.

Show your work.

7.	[7] This is frequency data from a long ciphertext, rounded to the nearest percent:												
	13	7	6	6	1	- ··- 3	2	8	·_·	4	2	2	0
	- 9	_· 7	_···	_··· 1	0	·- 1	-·- 3	· _·- 2	2	 2	 0	0	 8
	This is the start of the ciphertext: crack it.  ROUGH WORK												
			• •		• - •	• • • -	·	•	·	•-	• -•-		· · ·_··
	•	•• -			_•• _	•					٠		
	FINAL ANSWER												
	•	•• -			_·· _	•					·		
8.	[7] To find Vigenere ciphertext keylength, the Babbage/Kasiski method finds repeated and the offsets, eg. 19 35 28 24 42 63. For this example the most likely keylength is and the number of false positives is By contrast, the Friedman method, for each guess of the												
	keyle each	ength,	comp	outes t	to						_ of ea	ch of	the resulting: if et, otherwise each value should be

9.	[5]		_, the au	, the author of our text, starts his story in										
	(circle					1786			the	trial	of			
					(A),	whose	crypto	system	was	an	en-			
	hanced					substit	ution	cipher.	Ur	nfortun	ately			
	$\underline{\hspace{1cm}}$ 's secretary $\underline{\hspace{1cm}}$ (B)													
	had read	widely o	n crypto	graphy,	and em	ployed _					(C)			
	as a cod	e cracker	and G	ifford to	smugg	le letters	between	n (A) ai	nd the	conspin	rator			
				(.	D). (A)	was tricke	ed into re	evealing t	the co-c	onspira	tors:			
	(B) had (C) forge an encrypted to a letter from (D) to (A) that asked													
	for their names.													
10.	[5] Fathe	er and s	on				(A	A) becar	ne cry	ptograp	ohers			
	for the king of (B). In (circle one) 1526 1626 1726 1826 1896													
	the father cracked a message revealing that an army trapped inside a city was													
					(AA) de	esigned a	special	cipher fo	r (B) tl	hat was	s not			
	cracked until (circle one) 1526 1626 1726 1826 1896. This cipher had about (circle one)													
	50 150 30	0 450 600					characte	rs: it was	s first th	ought t	to be			
	a				cipher,	but was	a							
	cipher. A	fter the o	eipher wa	as cracke	ed, secret	correspo	ondence o	of (B) su	ggested	an ide	ntity			
	of													
11.	[4] The _													
	In the year a German u-boat sank the passenger ship													
	Lusitania, with about people on board. A telegram from (A) to the													
	America. The country of (B) suggested that (B) join the war again cracked the telegram: a													
	America.	The co	untry of					cracked	the te	legram:	: af-			
	ter giving the decryption to the Americans, they managed to keep secret the fact that													