

1. (15pts) Fill in the blanks: An encryption algorithm can be used to provide confidentiality in a communication. The information source, or plaintext, clear text is given as input to the cipher, together with a secret (encryption, private) key. The output of the encryption algorithm is called ciphertext (only this option).
2. (12 pts) Use the correct choice to fill the blank:
- a. (4 pts) Cryptanalysis, ***** { Cryptanalysis, Cryptography } is the name given to the study of techniques to circumvent encryption algorithms.
 - b. (4 pts) A mono-alphabetic cipher may ***** { may, may not } be readily broken by using frequency analysis of the characters in ciphertext samples.
 - c. (4 pts) The key to a Hill cipher can be found if the attacker solves linear equations derived from plaintext-ciphertext pairs { performs frequency analysis on ciphertext-only data, solves linear equations derived from plaintext-ciphertext pairs }.
- 3 (13pts) Draw the square diagram for the Playfair cipher with the keyword “spylove” and encrypt the sentence “falsetruce”.

8pts				
S	P	Y	L	O
V	E	A	B	C
D	F	G	H	I/J
K	M	N	Q	R
T	U	W	X	Z

Falsetruce = FA LS ET RU CE → GE OP VU MZ VA (5pts)

- 4 (10pts) The following is a small ciphertext sample encoded with a Vigenère cipher. Guess the keyword length using the Kasiski method for character trigrams.

“PPRESMREVTGGSFLEVTK” : keyword is seven characters long.