ID: _____

Name: KEY

Section: _1__

ITCS 412 Cryptography
Second semester 2007/2008
Quiz 2 – Classical Ciphers
Date: Mon. 25/3/2008

Q1. Fill in the blank with an appropriate word or number.

1) Cryptology is a science which includes as its branches: cryptography, cryptanalysis and steganography. (1)
2) In a known plaintext attack the cryptanalyst knows ....a....pair....of..... plaintext...and...the...corresponding...ciphertext. (1) (1) (1)
3) Both ...Kasiski..... and ...Babbage..... discovered independently a method for breaking the Vigenere ciphers.
4) A cipher which encrypts one byte (or one bit) at a time is called a ....stream.. cipher. (1)
5) An example of an unconditionally secure cipher is ....one-time pad..... (1)

Q2. Construct the encryption matrix for the Playfair cipher using the key SHAKE. Then encrypt the word 'includes'. (4)

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