Computer Security Homework 1 (Due Friday 8/21/20)

1. Encrypt the message CRYPTO using a substitution cipher with the key given below.

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

2. Encrypt the message ILOVEZOOM using the Vigenère cipher with the key BASE. Assume A is a shift by 0, B is a shift by 1, etc.

3. Encrypt the message CAT with a one-time pad whose key is $(1, 24, 4)$.

4. The message below was encrypted with a substitution cipher. Decrypt it. There are online tools for this, but it's more fun to try it without one.

```
JA VDA QACQLA CI VDA UESVAB FVPVAF, SE CWBAW VC ICWG P GCWA QAWIAXV
UESCE, AFVPRLSFD OUFVSXA, SEFUWA BCGAFVSX VWPEZUSLSVK, QWCNSBA ICW
VDA XCGGCE BAIAEXA, QWCGCVA VDA TAEAWPL JALIPWA, PEB FAXUWA VDA
RLAFFSETF CI LSRAWVK VC CUWFALNAF PEB CUW QCFVAWSVK, BC CWBPSE PEB
AFVPRLSFD VDSF XCEFVSVUVSCE ICW VDA UESVAB FVPVAF CI PGAWSXP.
```

5. The message JAVA was encrypted with a one-time pad into LRUW. You obtain the ciphertext YFGG of another message encrypted with the exact same key. What must that message say? Show your work. [Hint: The text should decrypt into readable English.]

6. One-time pads are the only provably unbreakable system. Why aren't they used more often?

7. A one-time-pad is used to encrypt a message into DSUVWENABXOZ. Someone claims that the key must have been [3, 25, 1, 21, 20, 20, 13, 7, 24, 23, 18, 12] since that decrypts the message into ATTACKATDAWN. How likely is that person to be right? Explain.

8. Suppose we encrypt a message with a substitution cipher with a given key and then encrypt that ciphertext with a substitution cipher with another key. Is this approach (a) twice as secure as a single substitution cipher or (b) no more secure than a single substitution cipher? Explain.