2. (6 pts) Decrypt the following message, which was enciphered using the Atbash cipher.

RGWLV HMLGN ZGGVI SLDHO LDOBB LFTLH LOLMT ZHBLF WLMLG HGLK

3. (a) (5 pts) The MOD BAAAAA cipher with keyword MOVIE was used to produce the ciphertext

ZNGMJ FUJWX

Decipher the message.

(b) (5 pts) A ciphertext encrypted with Vigen'ere contains four occurrences of the letter sequence WCTAWWI starting at positions 258, 270, 378 and 454. What is the probable length of the key? Explain.

4. (a) (4 pts) Write $t = 17721$ as a sum of a subset of the superincreasing sequence

$$47, 52, 112, 216, 436, 868, 1732, 3470, 6937, 13876$$

(b) (6 pts) Use the Euclidean algorithm to find gcd(8191, 255).

5. Alice and Bob use base twenty-six encoding and RSA. Alice's public modulus is $m_A = 3403$ and her encryption exponent is $e_A = 17$. Bob's public modulus is $m_B = 7747$ and his public exponent $e_B = 23$.

   (a) (6 pts) Find Alice's decryption exponent d_A. Make sure to **verify** your answer!

   (b) (6 pts) Alice receives the *enciphered* message-signature pair $(\tilde{x}, \tilde{\sigma}) = (2819, 1329)$. Recover the encoded message x and its signature σ.

(c) (4 pts) Verify that the above pair was sent by Bob.

(d) (4 pts) Decipher Bob's plaintext (**Note**: Your answer should be an English word).

6. (10 pts) The following text was encrypted using a keyword to obtain a mixed alphabet.

BAIRM RHTBN JMEIQ BPIIR HTBMI GIGOI MBTJR HTBSH TIMPQ RHT

The last word of the plaintext is "UNDERSTAND". Decrypt the message and recover the keyword. Show all your work and explain your method.

plain	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
cipher																										

7. (10 points) The ciphertext

```
EAOEV STSMG IYESS ARNCH BTFDO ISTOI AREID RRUMW TOLVM IEEHR AEOOE R
```

was produced by a keyword columnar transposition using a seven-letter keyword. Recover the plaintext assuming it contains the word "OBVIOUS".

8. (10 points) Suppose that "DARK KNIGHT" enciphers as "PYHY YPOCJH" by using the Hill cipher with a 2×2 matrix A. Determine A and use the same Hill cipher to decipher "FIRCAN".

9. The following three ciphertexts

```
XMEEQ IVAVZ POFBK SOWPI LGUCH AHKEI WGMGV XASRL ZT,

ERHGS SAYTT EOSSV YIHIB UBNER NEIET NATET UOVYE ET,
```

and

```
ZQZMT OCDIB CVNDO NWZVP OTWPO IJOZQ ZMTJI ZNZZN DO
```

came from the same plaintext.

(a) (6 pts) One of the ciphertexts was enciphered using a shift cipher, one came from a Vigenère encipherment with a 13-letter keyword and the other came from a simple columnar transposition. Find which is which. *Explain* your answers.

(b) (6 pts) Find the plaintext.