Solutions

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

RGWLV HMLGN ZGGVI SLDHO LDOBB LFTLH LOLMT ZHBLF WLMLG HGLK

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

ITDOESNOTMATTER HOW SLOWLY YOU GO SO LONG AS YOU DO NOT STOP.

not tested in our course

It does not matter how slowly you go, so long as you do not stop.

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

ZNGMJ FUJWX

Decipher the message.

Not in our course

(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.

$270 - 258 = 12$

$378 - 258 = 120$ $\quad 378 - 270 = 108$

$454 - 378 = 76$ $\quad 454 - 258 = 196$

$\gcd(12, 120, 76, 108, 196) = 4$, so the Kasiski Test tells us the length of the keyword is either 2 or 4. It is probably 4, as a keyword of length 2 is less likely.

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

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

17721 > 13876, so include it

3845 left

3845 > 3470, so include it

375 left

Include 216

159 = 47 + 112 left

$$17721 = 13876 + 3470 + 216 + 112 + 47$$

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

$$8191 = 32 \cdot 255 + 31$$

$$255 = 8 \cdot 31 + 3$$

$$31 = 10 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

$$\gcd(8191, 255) = 1$$

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!

$m_a = 3403 = 41 \cdot 83$

$n_a = 40 \cdot 82 = 3280$

$3280 = 192 \cdot 17 + 16$

$17 = 16 + 1$

$1 = 17 - 16 = 17 - (3280 - 192 \cdot 17)$

$= 193 \cdot 17 - 3280$

$d = 193$

$e \cdot d \equiv 1 \pmod{3280}$ ✓

(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.

Not tested in this class

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

Can't do without (b)

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

Can't do without (b).

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

I EAR ANDI OR ETISEEA NDIREMEMBE RIDOA NDJUN DERST AND
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	R							H					M	P	Q	S										

O U N E A B C D F G J K L V W X Y Z

RE _ E _ _ ER

↑ ↑

Same letter, could be remember

B - one letter word between AND + Remember, so probably I

Decryption

I hear and I forget, I see and I remember. I do and I understand

Keyword

ROUTINE

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".

56 letters - 7 colums, 8 rows.

(7)	(4)	(6)	(5)	(3)	(1)	(2)
E	M	R	O	E	T	H
A	G	N	I	I	O	R
O	I	C	S	D	L	A
E	Y	H	T	R	V	E
V	E	B	O	R	M	O
S	S	T	I	U	I	O
T	S	F	A	M	E	E
S	A	D	R	W	E	R

We need the word "OBVIOUS" across a row, so we order the columns in that way. Also, OBVIOUS its 7 letters, so each letter is in a different column. Since O, B, V are the row above I, O, U, S, they must be the last 3 columns.

Plain text: The more original a discovery, the more obvious it seems afterwards.

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".

DARK KNIGHT
3 0 17 10 10 13 8 6 7 19

PYHY YPOCJH
15, 24, 7, 24 24, 15, 14, 2, 9, 7

Hill Cipher $y = A x \pmod{26}$, and A must be invertible mod 26.

We must pick 4 letters to create X so that X is invertible, since $A \equiv y \cdot x^{-1} \pmod{26}$.

$\begin{bmatrix} 3 & 17 \\ 0 & 10 \end{bmatrix}$ is not. $\begin{bmatrix} D & H \\ 3 & 7 \\ A & T \\ 0 & 19 \end{bmatrix}$ is.

$\begin{bmatrix} 3 & 10 \\ 0 & 3 \end{bmatrix}$ is not

So, we use $X \equiv \begin{bmatrix} 3 & 7 \\ 0 & 19 \end{bmatrix} \pmod{26}$ & $Y \equiv \begin{bmatrix} 15 & 9 \\ -2 & 7 \end{bmatrix}$

$$X^{-1} \equiv 5^{-1} \begin{bmatrix} 19 & -7 \\ 0 & 3 \end{bmatrix} \equiv 21 \begin{bmatrix} -7 & -7 \\ 0 & 3 \end{bmatrix} \equiv \begin{bmatrix} 9 & 9 \\ 0 & 11 \end{bmatrix} \pmod{26}$$

$$A \equiv \begin{bmatrix} 15 & 9 \\ -2 & 7 \end{bmatrix} \begin{bmatrix} 9 & 9 \\ 0 & 11 \end{bmatrix} \equiv \begin{bmatrix} -99 & -99+99 \\ -18 & -18+77 \end{bmatrix} \equiv \begin{bmatrix} 5 & 0 \\ 8 & 7 \end{bmatrix} \pmod{26}$$ A

$$A^{-1} \equiv 9^{-1} \begin{bmatrix} 7 & 0 \\ -8 & 5 \end{bmatrix} \equiv 3 \begin{bmatrix} 7 & 0 \\ -8 & 5 \end{bmatrix} \equiv \begin{bmatrix} -5 & 0 \\ 2 & 15 \end{bmatrix} \pmod{26}$$

FIRCAN A^{-1} decryption

$$X \equiv \begin{bmatrix} -5 & 0 \\ 2 & -11 \end{bmatrix} \cdot \begin{bmatrix} 5 & 17 & 0 \\ 8 & 2 & 13 \end{bmatrix} \equiv \begin{bmatrix} 1 & 19 & 0 \\ 2 & 12 & 13 \end{bmatrix} \pmod{26}$$

BATMAN

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.

① Vigenere - No letter is significantly more frequent than others

② Transposition - Most frequent letters are the most frequent in English (E, T, N, S)

③ Shift. Some letters (O, Z) much more frequent than others

(b) (6 pts) Find the plaintext.

from comparing 2nd + 3rd, Plain E→Z, T→O, so a shift of -5 to encrypt, so shift +5 to decrypt!

EVERY THING HAS ITS BEAUTY BUT NOT EVERY ONE SEES IT.