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

Q1)

Plaintext:

THISIS ...

Q2) The Vigenère cipher has a keyword, such as SESAME

A plaintext such as

EVERYONEHATESEXAMS

over a 26-letter A-Z is enciphered as follows:

EVERYONEHATESEXAMES
SESAMESESAMESESAMES
IN Z .- - - - - -

Ciphertext

A_LONG_LONG_TIME_AGO_

EM

ZHWWEKKWWZKKDQD

Q3)

Either:

~~frequency analysis can't be used over short messages~~

~~OR~~

A Vigenère cipher has a large keyspace and so an exhaustive search of keys can't be applied.

Q4) In the enigma cipher the i-th letter X of plaintext is enciphered as

$$f(X, i)$$

where f is a non-linear function of X and i, so frequency analysis

Can't be used.

Q5

$f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad x \longmapsto 9x + 16$

$f^{-1} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad x \longmapsto 9^{-1}(x - 16)$

$= 3(x - 16)$

$= 3x + 4$

$f^{-1}(T) = f^{-1}(19)$

$= 3(19) + 4$

$= 3(-7) + 4$

$= -17$

$= 9$

$= J$

$f^{-1}(M) = \cdots$

$f^{-1}(Y) = \cdots$

Q6

$$A = \begin{pmatrix} 2 & 3 \\ 7 & 5 \end{pmatrix}$$

$$A^{-1} = (\det A)^{-1} \begin{pmatrix} 5 & -3 \\ -7 & 2 \end{pmatrix}$$

$$= (-11)^{-1} \begin{pmatrix} 5 & -3 \\ -7 & 2 \end{pmatrix}$$

$$= 15^{-1} \begin{pmatrix} 5 & -3 \\ -7 & 2 \end{pmatrix}$$

$26 = 15 + 11$

$15 = 11 + 4$

$11 = 2.4 + 3$ ✓

$4 = 3 + 1$ ✓

$1 = 4 - 3$

$= 4 - (11 - 2.4) = 3.4 - 11$

$= 3.(15 - 11) - 11 = 3.15 - 4.11$

$= 3.15 - 4(26 - 15) = 7.15 - 4.26$

$\equiv 7.15$

$$A^{-1} = 7 \cdot \begin{pmatrix} 5 & -3 \\ -7 & 2 \end{pmatrix}$$

$$\begin{pmatrix} E \\ S \end{pmatrix} \mapsto 7 \begin{pmatrix} 5 & -3 \\ -7 & 2 \end{pmatrix} \begin{pmatrix} 4 \\ 18 \end{pmatrix} = \begin{pmatrix} W \\ E \end{pmatrix}$$

$$\begin{pmatrix} D \\ C \end{pmatrix} \mapsto \begin{pmatrix} A \\ L \end{pmatrix}$$

$$\begin{pmatrix} D \\ O \end{pmatrix}$$

$$\begin{pmatrix} N \\ E \end{pmatrix}$$