CS 402 Cryptography

Problem Sheet 3

(1) Calculate $\varphi(1001)$ and $\varphi(5040)$, where φ is the Euler totient function.

(2) Show that the number of encryption keys (a, b) for an affine cryptosystem with encryption function $x \mapsto ax + b \mod N$ is equal to $N^2 - N$ if and only if N is prime.

(3) Encrypt the message GOODLUCK using length 2 message units and the affine matrix encryption $X \mapsto \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} X$, where the alphabet is $\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}$.

(4) You intercept the ciphertext ZRIXXYVBMNPO which was encrypted using an affine matrix cryptosystem with length 2 message units and a 27-symbol alphabet $\mathrm{A} = \emptyset, \ldots, \mathrm{Z} = 25$, $\square = 26$ (where $\square$ stands for a space). Frequency analysis shows that the most commonly occurring units in earlier ciphertexts are PK and RZ. You guess that these correspond to the most frequently occurring plaintext units in the alphabet, namely E$\square$ and S$\square$, respectively. Find the decryption matrix and decrypt the ciphertext.

(5) You intercept ciphertext !IWGVIEX!ZRADRYD which was encrypted using an affine matrix encryption $X \mapsto \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} X$ and length 2 message units, working over the 29-symbol alphabet $\mathrm{A} = \emptyset, \ldots, \mathrm{Z} = 25$, $\square = 26$, $? = 27$, $! = 28$, where $\square$ stands for a space. The last five letters of the plaintext are MARIA. Decrypt.