

Ex:- You intercept the ciphertext
 "PHULPZTQAHF", which you know was
 encrypted using an affine map on digraphs in
 26-letter alphabet. An extensive statistical
 analysis of earlier ciphertexts which had
 been coded by the same enciphering map
 shows that the most frequently occurring
 digraphs in all of that ciphertext are
 "IX" and "TQ", in that order. It is
 known that the most common digraphs in
 the English Language are "TH" and "HE",
 in that order. Read the message.

$$C \equiv aP + b \pmod{N^2} \rightarrow \text{encryption scheme.}$$

$$\begin{array}{l|l} IX \Rightarrow 26 \times 8 + 23 = 231 & TH \Rightarrow 26 \times 19 + 7 = 501 \\ TQ \Rightarrow 26 \times 19 + 16 = 510 & HE \Rightarrow 26 \times 7 + 4 = 186 \end{array}$$

$$P \equiv a^{-1}C - a^{-1}b$$

$$\Rightarrow \left. \begin{array}{l} 501 \equiv 231a^{-1} - a^{-1}b \\ 186 \equiv 510a^{-1} - a^{-1}b \end{array} \right\} \text{Subtracting} \Rightarrow$$

$$\Rightarrow 279a^{-1} \equiv -315 \equiv 361 \pmod{26^2}$$

$$\begin{aligned} \therefore a^{-1} &\equiv 361 \times 279^{-1} \pmod{676} \\ &\equiv 361 \times 63 \equiv \underline{\underline{435}} \pmod{676} \end{aligned}$$

$$\begin{aligned}\text{Now } -a^{-1}b &= 501 - 231a^{-1} \\ &= 501 - 231 \times 435 \equiv 64 \pmod{676}\end{aligned}$$

\therefore Decryption Scheme:

$$\begin{aligned}P &\equiv a^{-1}c - a^{-1}b \\ \Rightarrow P &\equiv 435C + 64 \pmod{676}\end{aligned}$$

$$\begin{array}{lcl}PW \Rightarrow 26 \times 15 + 22 = 412 & \rightarrow & P = 144 = 26 \times 5 + 14 \\ VL \Rightarrow 26 \times 20 + 11 = 531 & \rightarrow & = 533 = 26 \times 20 + 13 \\ PZ \Rightarrow 26 \times 15 + 25 = 415 & \rightarrow & 97 = 26 \times 3 + 19 \\ TQ \Rightarrow 26 \times 19 + 16 = 510 & \rightarrow & 186 = 26 \times 7 + 4 \\ AW \Rightarrow 26 \times 0 + 22 = 22 & \rightarrow & 170 = 26 \times 6 + 14 \\ HF \Rightarrow 26 \times 7 + 5 = 187 & \rightarrow & 289 = 26 \times 11 + 3\end{array}$$

Required plaintext is "FOUNDTHEGOLD"