

Ex:- You intercept the cipher-text  
 "APHWULPZTQAWHF", which you know was  
 encrypted using an affine map on digraphs in  
 26-letter alphabet. An extensive statistical  
 analysis of earlier ciphertext 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.

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

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

$$\begin{aligned} P &\equiv \bar{\alpha}^{-1}C - \bar{\alpha}^{-1}b \\ \Rightarrow 501 &\equiv 231\bar{\alpha}^{-1} - \bar{\alpha}^{-1}b \quad \left. \right\} \text{Subtracting } \\ 186 &\equiv 510\bar{\alpha}^{-1} - \bar{\alpha}^{-1}b \end{aligned}$$

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

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

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

$\therefore$  Decryption Scheme:

$$P = a^{-1}c - a^{-1}b \\ \Rightarrow P = 435c + 64 \pmod{676}$$

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

Required plaintext is "FOUND THE GOLD"