Polyalphabetic ciphers (a.k.a Renaissance Cipher)

➡ Vigenere cipher

Algorithm : combine the message and the key

Key : a word

Key space : the length of the word

$$\begin{array}{rl} & \texttt{wearediscoveredsaveyourself} \\ + & \texttt{deceptivedeceptivedeceptive} \pmod{26} \\ \hline & \texttt{ZICVTWQNGRZGVTWAVZHCQYGLMGJ} \end{array}$$

Advantage : Encryption of a letter is context dependent

Breaking Polyalphabetic Ciphers