

Polyalphabetic ciphers (a.k.a Renaissance Cipher)

➔ Vigenere cipher

Algorithm : combine the message and the key

Key : a word

Key space : 26^n (n being the length of the key)

wearediscoveredsaveyourself	
+ <u>deceptivedeceptivedeceptive</u>	(mod 26)
ZICVTWQNGRZGVTWAVZHCQYGLMGJ	

Advantage : Encryption of a letter is context dependent

Breaking Polyalphabetic Ciphers