Breaking Caesar cipher

Exhaustive search

ciphertext only

known plaintext

chosen plaintext

chosen ciphertext

Exhaustive search

ciphertext only

known plaintext

chosen plaintext

chosen ciphertext

Yes
Statistical Analysis
Look at the first letter and get the shift
Choose “A” and get the shift
Choose “A” and get the shift

Breaking Caesar cipher

Exhaustive search	Yes
ciphertext only	Statistical Analysis
known plaintext	Look at the first letter and get the shift
chosen plaintext	Choose “A” and get the shift
chosen ciphertext	Choose “A” and get the shift

Statistical Cryptanalysis

- Monoalphabetic ciphers do not change the relative frequency of letters in a message