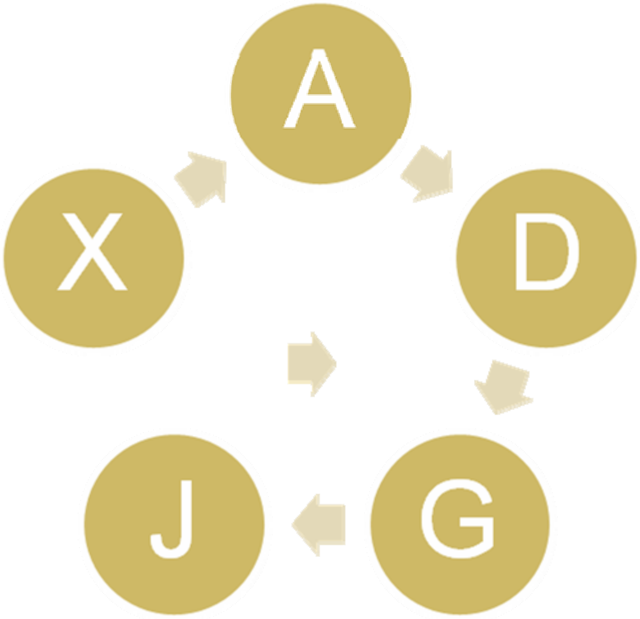
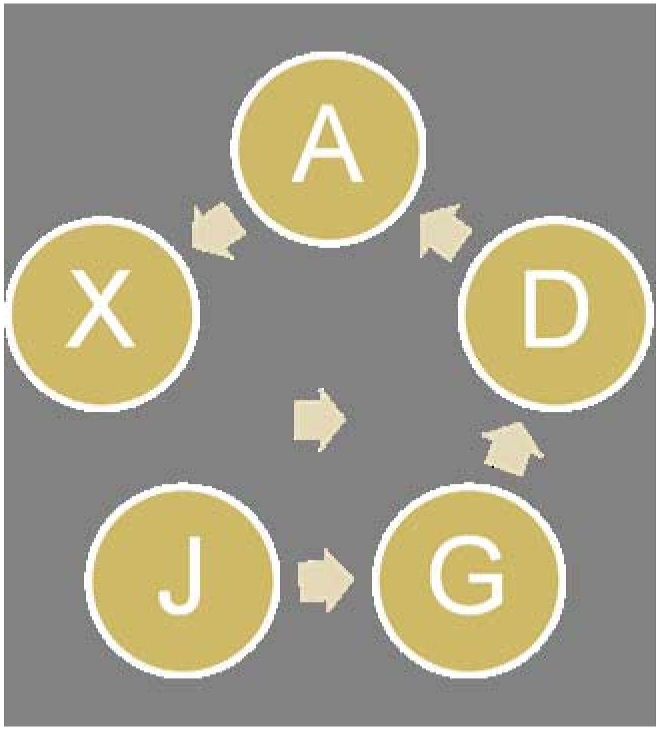
SHIFT CIPHER

- Rotate each letter by the key k
- For example, if k is 3 then:



Encryption

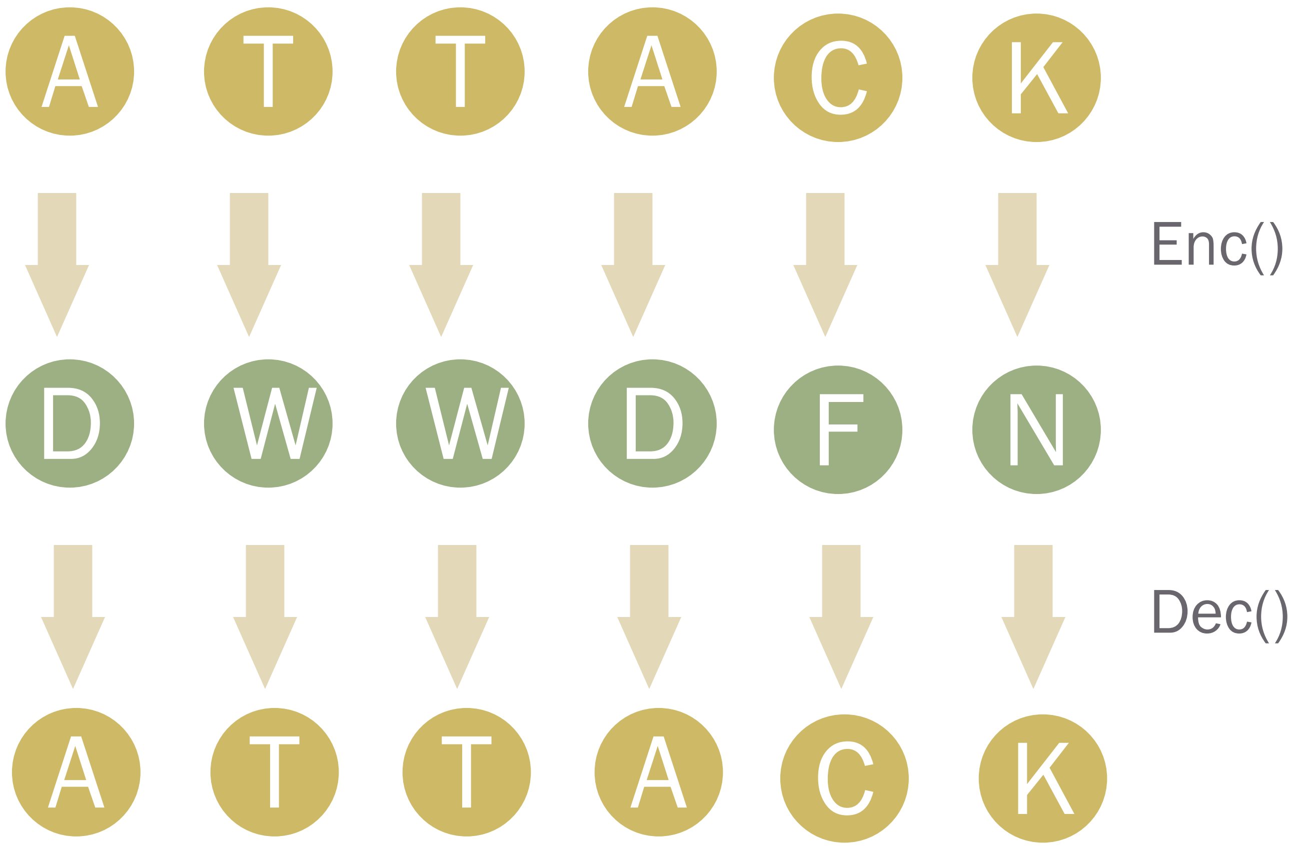
Enc(x) = (x + k) mod 26.



Decryption

Dec(x) = (x - k) mod 26

Example: Key = 3 and Plaintext = “ATTACK”



A T T A C K

Enc()

D W W D F N

Dec()

A T T A C K

Problem with Shift ciphers

- Not enough keys!
- If we shift a letter 26 times, we get the same letter back.
  - A shift of 27 is the same as a shift of 1, etc.
  - So we only have 25 keys (1 to 25).
- Therefore, easy to attack via brute force.

Example: Cryptanalysis of shift ciphers

- Cipher text : OVDTHUFWVZZPISLRLFZHYLAOLYL

Key Value	Possible Plain Text
1	NUCSGTEVUYYOHRKQKEYGXKZNKXK
2	MTBRFSDUTXXNGQJPJDXFWJYMJWJ
3	LSAQERCTSWWMFPIOICWEVIXLIVI
4	KRZPDQBSRVVLEOHNHBVDUHWKHUH
5	JQYOCPARQUUKDNGMGAUCTGVJGTG
6	IPXNBOZQPTTJCMFLFZTBSFUIFSF
7	HOWMANYPOSSIBLEKEYSARETHERE
8	GNVLZMXONRRHAKDJDXRZQDSGDQD
9	FMUKYLWNMQQGZJCICWQYPCRFCPC
10	ELTJXKVMLPPFYIBHBVPXOBQEBOB
11	DKSIWJULKOOEXHAGAUOWNAPDANA
12	CJRHVITKJNNDWGZFZTNVMZOCZMZ
13	BIQGUHSJIMMCVFYEYSMULYNBYLY