Substitution Cipher

$A \to D$
$B \to E$
$C \to F$
$\vdots$
$Z \to C$

Shift, Affine:
One-to-one functions with domain & range $\{0, 1, 2, \ldots, 25\}$

Shift $f_k(x) = (x+k) \bmod 26$
Affine $f_{a,b}(x) = (ax+b) \bmod 26$

Another way to define a function is to explicitly list each output for each input!
(Can only do this if there aren't too many inputs)

Plain	Cipher
A	Q
B	R
C	C
D	Z
E	B
⋮	

each letter must appear here exactly once!!!

$26 \times 25 \times 24 \times \cdots \times 1$

$26! \approx 10^{26}$ bits

Shift key size = 26
Affine = $12 \times 26 = 312$

Key size =

NOT FEASIBLE TO DO A BRUTE FORCE SEARCH!!!

	Shift/Affine	Substitution
Pro	easy to implement	Large keyspace
Con	Small Keyspace	harder to implement (probably need to carry a chart)

Hiding the fact that you've sent a message is steganography.

Substitution cipher was used as well, just in case!!!

Queen Elizabeth's Cipher Person: Francis Walsingham

Some words are really common (the, etc.)

CODE SYMBOLS for 20 common words.

The - △

26 letters +
20 symbols (harder)
3/4 null chars

Other Things to Make Harder

NULL ~~SKIP~~ CHAR (doesn't count)
BACKSPACE CHAR

How did Walsingham Break the Code? (3)

(1) Frequency Analysis
- Calculate all letter frequencies
- 1st 5 or so probably map to the 1st 8 or so from regular English frequencies

(2) Common Di, Tri grams
- Try to match repeated di-tri grams in the ciphertext to common ones in English.
- Plug in ideas and see if "impossible" conditions are created, OR if a partial word forms.

(3) Repeated Words
- match "mold" of word to dictionary.

XYXXZ = daddy