Attacks

m plaintext
c ciphertext

What Eve has access to:

- ciphertext only attack — only c
- known plaintext attack — also: some pair $(\tilde{m}, \tilde{c})$
- chosen plaintext attack — can compute $E(\tilde{m}) = \tilde{c}$ for some $\tilde{m}$
- chosen ciphertext attack — can compute $D(\tilde{c}) = \tilde{m}$ for some $\tilde{c}$

historical ciphers not secure even against ciphertext only attacks
[under known plaintext attacks, they fall apart entirely]

EG $c = BKNDKGBQ$

somehow Eve learns that Vigenere is used and that

$m = ALLCLEAR$

recall: $m + k$ "=" c — characterwise mod 26, repeat k

$\longrightarrow$ k "=" $c - m$

substitution cipher — k permutation of alphaSet

EG $k = FRA\ldots$ encrypt $A \to F$, $B \to R$, $C \to A$, ..

How many possible keys? $26! \approx 10^{26.6} \approx 2^{88.4}$

$26! = 26 \cdot 25 \cdot \ldots \cdot 2 \cdot 1$

89 bits to store k, large!

DES: 56 bits

still easy to break: **frequency attack**

letter frequencies for English

E	T	A	O	...
12.7%	9.1%	8.2%	7.5%	

likewise digrams, trigrams, ...
TH, HE, ...