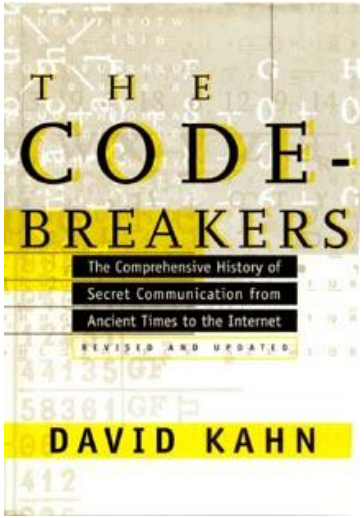
Introduction

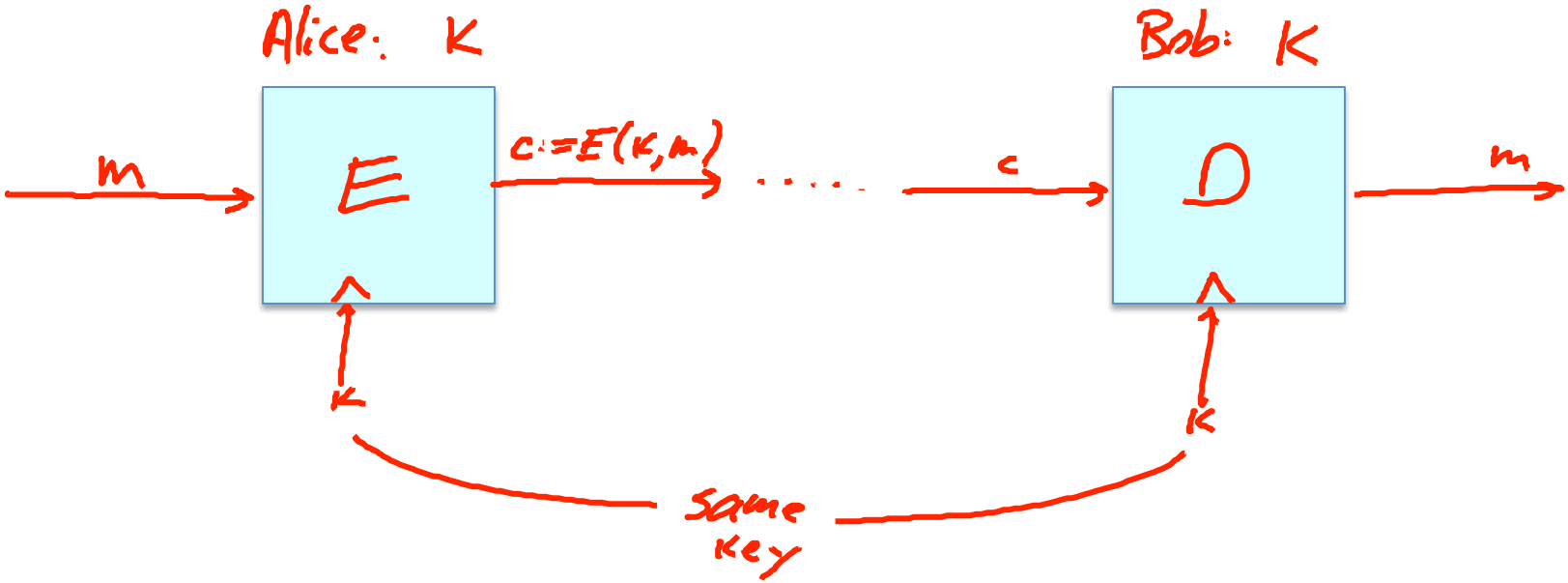
History

History

David Kahn, “The code breakers” (1996)



Symmetric Ciphers



Few Historic Examples (all badly broken)

1. Substitution cipher

$c := E(k, \text{"bcza"}) = \text{"wnac"}$

$D(k, c) = \text{"bcza"}$

k :=

$a \rightarrow c$
$b \rightarrow w$
$c \rightarrow n$
$\vdots$
$z \rightarrow a$

Caesar Cipher (no key)

shift by 3 :

a → d
b → e
c → f
⋮
y → b
z → c

What is the size of key space in the substitution cipher assuming 26 letters?

$|\mathcal{K}| = 26$

$|\mathcal{K}| = 26!$ (26 factorial)

$|\mathcal{K}| = 2\uparrow 26$

$|\mathcal{K}| = 26\uparrow 2$

$26! \approx 2^{88}$

How to break a substitution cipher?

What is the most common letter in English text?

"X"

"L"

"E"

"H"

How to break a substitution cipher?

(1) Use frequency of English letters

"e": 12.7%, "t": 9.1%, "a": 8.1%

(2) Use frequency of pairs of letters (digrams)

"he", "an", "in", "th"

$\Longrightarrow$ CT only attack!!

An Example

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYYFVUFO
FEIKNWFRFIKJNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHXCYBOHOPYXPUBNCUBOYNRVNIWN
CPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCYZPUKBZPUNVPWPCYVF
ZIXUPUNFCPWRVNBCVBRPYYNUNFCPWWJUKBYBIPOUZBCUIPOUNVNIPUBRNCHOPYXPUBNCUB
OYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZPUNVR

B	36
N	34
U	33
P	32
C	26

➔ E

➔ T

➔ A

NC	11
PU	10
UB	10
UN	9

digrams

➔ IN

➔ AT

UKB	6
RVN	6
FZI	4

trigrams

➔ THE

2. Vigener cipher (16'th century, Rome)

k = C R Y P T O C R Y P T O C R Y P T

(+ mod 26)

m = W H A T A N I C E D A Y T O D A Y

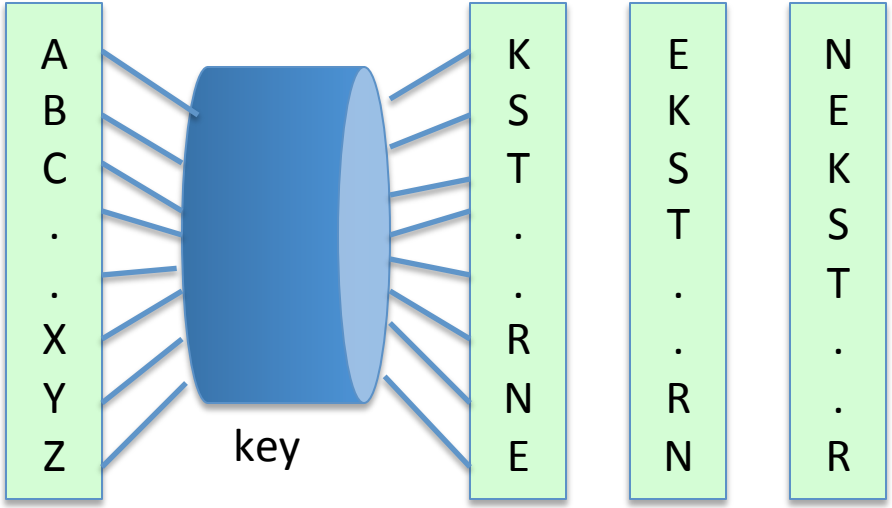
---

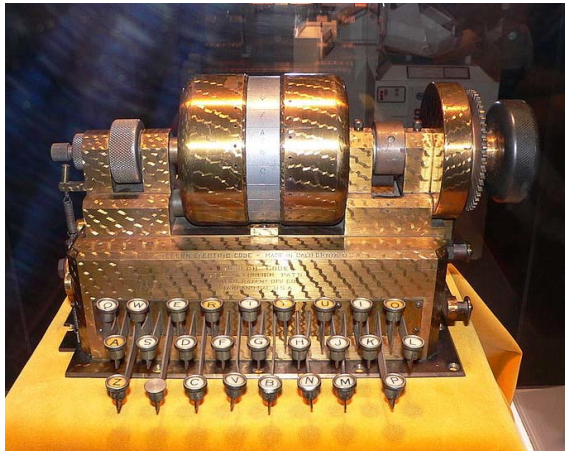
c = Z Z Z J U C L U D T U N W G C Q S

suppose most common = "H" ⟹ first letter of key = "H" – "E" = "C"

3. Rotor Machines (1870-1943)

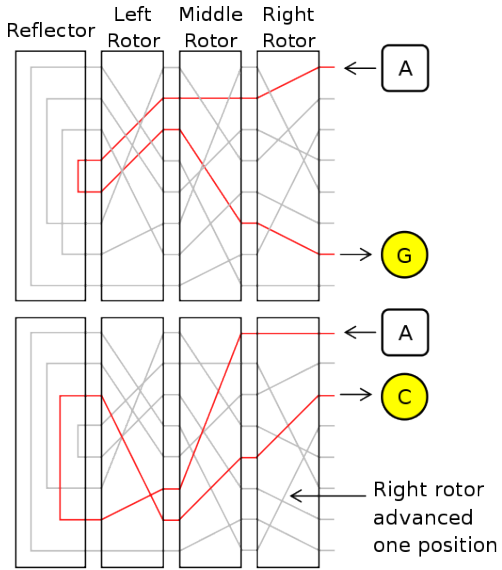
Early example: the Hebern machine (single rotor)





Rotor Machines (cont.)

Most famous: the Enigma (3-5 rotors)



keys = $26^4 = 2^{18}$ (actually 2^{36} due to plugboard)

4. Data Encryption Standard (1974)

DES: # keys = 2^{56} , block size = 64 bits

<u>Today</u>: AES (2001), Salsa20 (2008) (and many others)

End of Segment