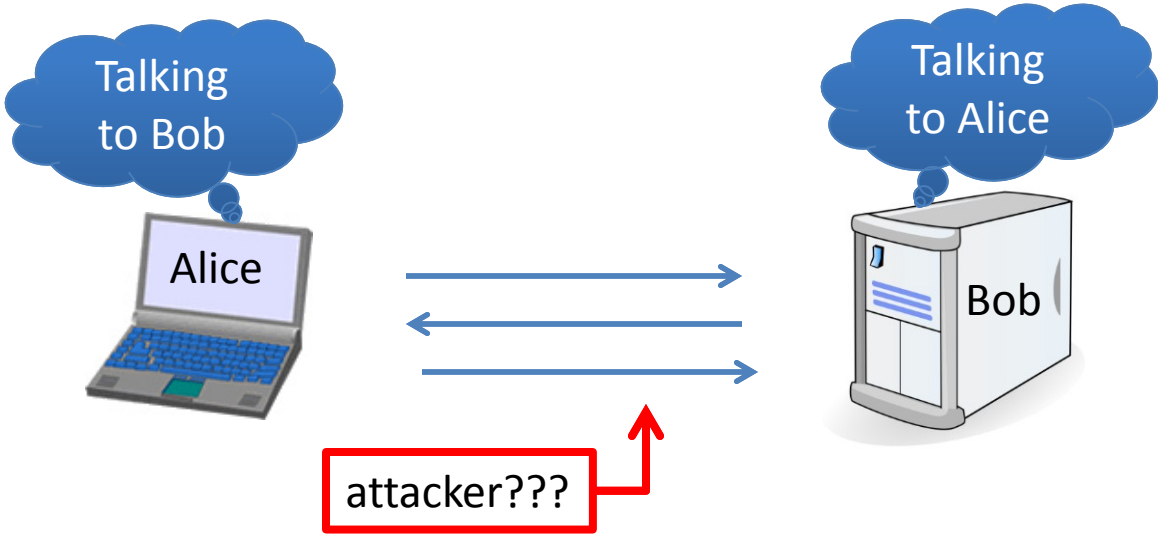

# Introduction

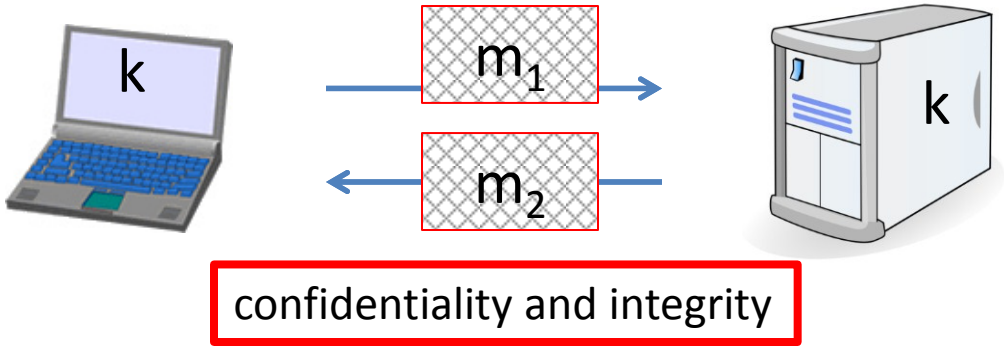
## What is cryptography?

# Crypto core

Secret key establishment:



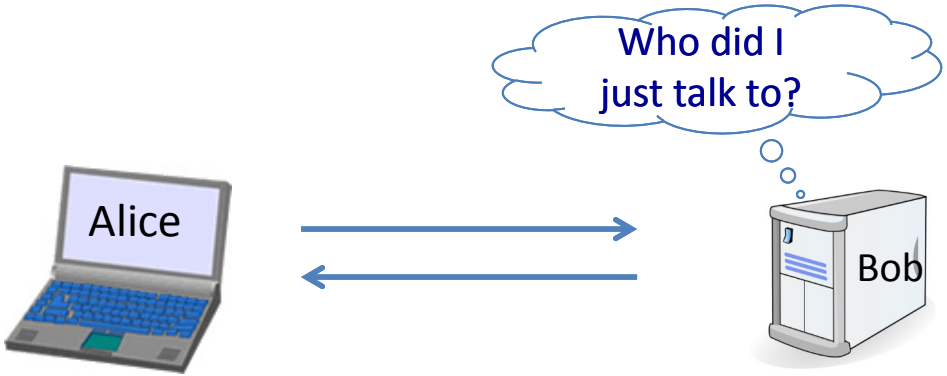

Secure communication:



# But crypto can do much more

- Digital signatures


- Anonymous communication

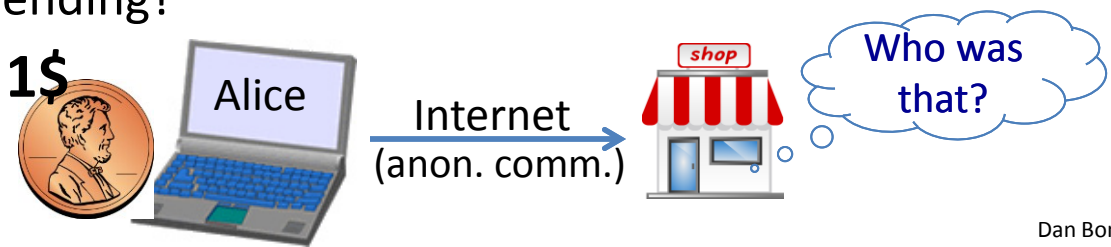


# But crypto can do much more

- Digital signatures

- Anonymous communication

- Anonymous **digital** cash
  - Can I spend a “digital coin” without anyone knowing who I am?
  - How to prevent double spending?

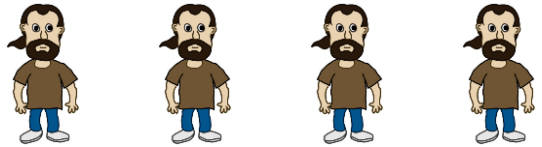


# Protocols

- Elections
- Private auctions

# Protocols

- Elections
- Private auctions



Goal: compute $f(x_1, x_2, x_3, x_4)$

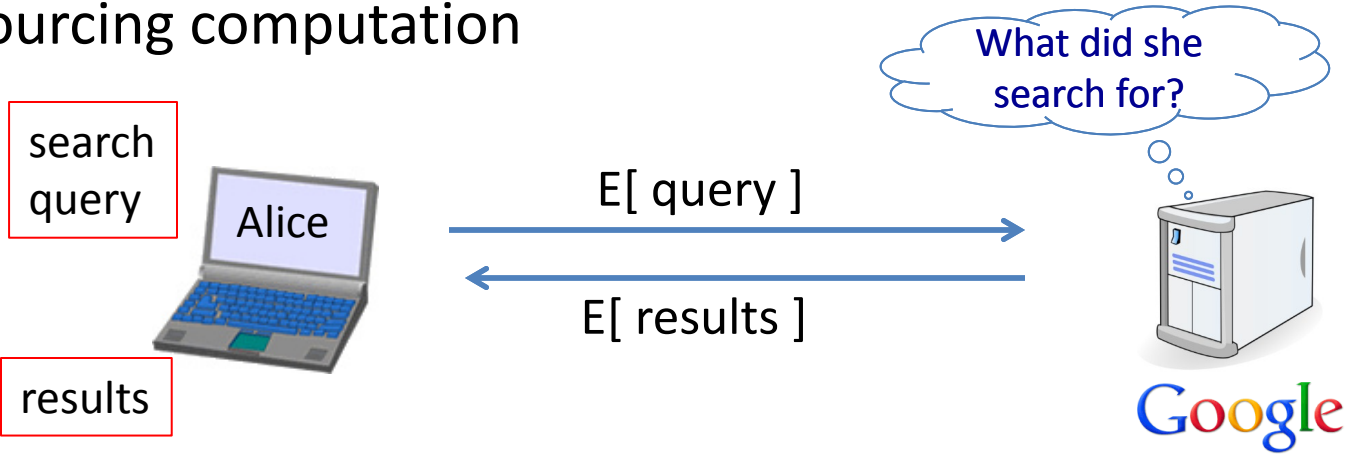
trusted authority

"Thm:" anything the can done with trusted auth. can also be done without

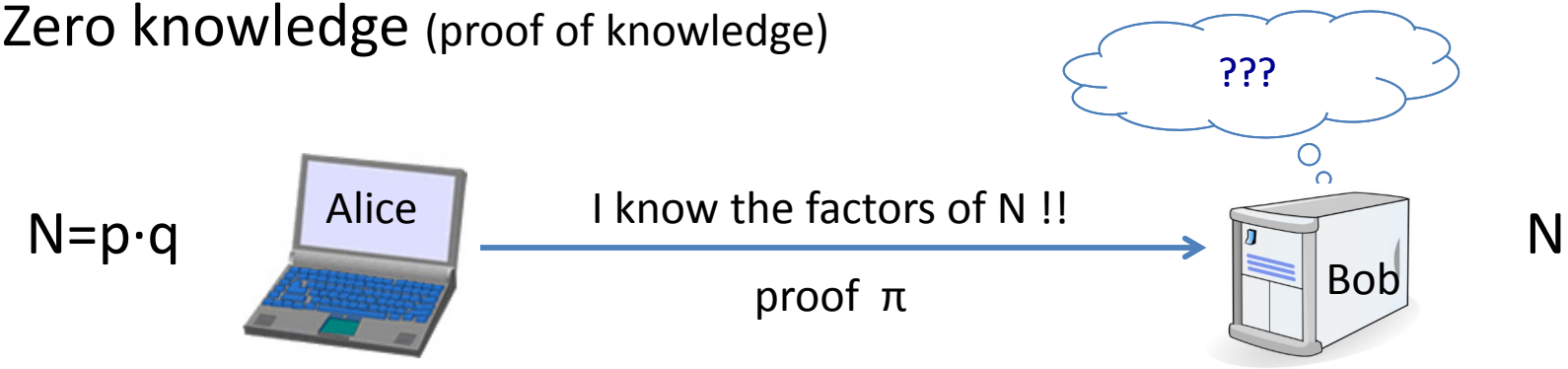
- Secure multi-party computation

# Crypto magic

- Privately outsourcing computation




- Zero knowledge (proof of knowledge)



# A rigorous science

The three steps in cryptography:

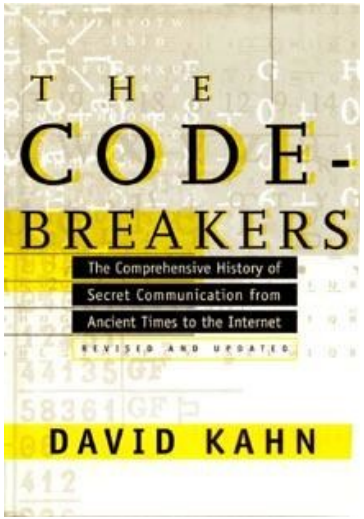
- Precisely specify threat model
- Propose a construction
- Prove that breaking construction under threat mode will solve an underlying hard problem


# Introduction

## History

# History

David Kahn, “The code breakers” (1996)

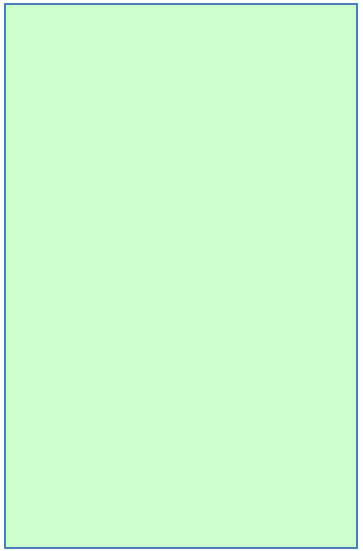


# Symmetric Ciphers

# Few Historic Examples (all badly broken)

1. Substitution cipher

k :=



# Caesar Cipher (no key)

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

$|\mathcal{K}| = 26$

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

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

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

# 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

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

# 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

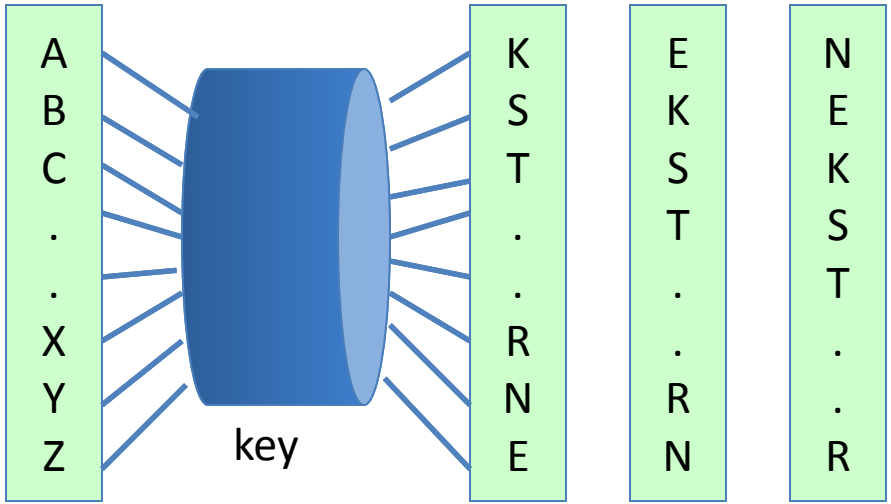
---

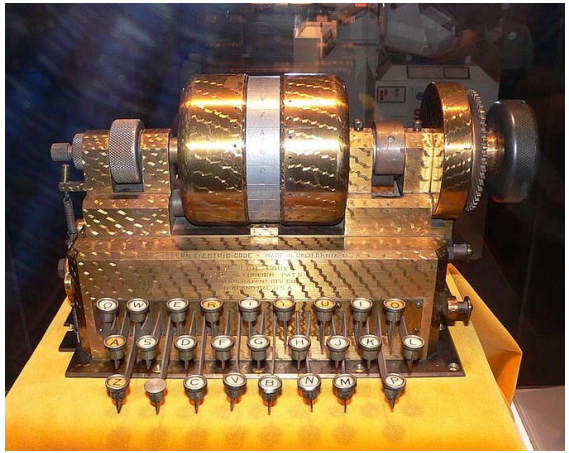
c = Z Z Z J U C L U D T U N W G C Q S

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

# 3. Rotor Machines (1870-1943)

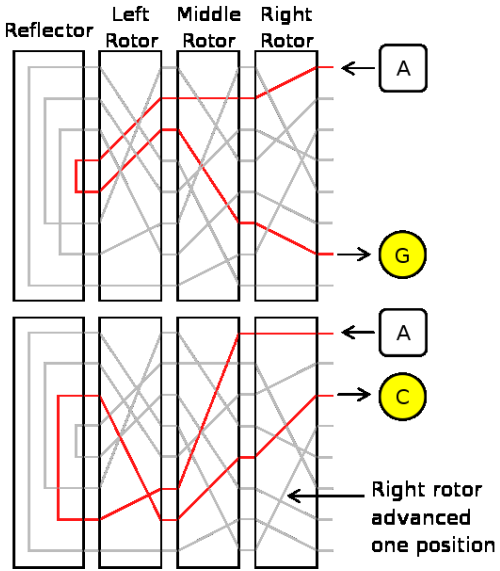
Early example: the Hebern machine (single rotor)



# 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

Today: AES (2001), Salsa20 (2008) (and many others)