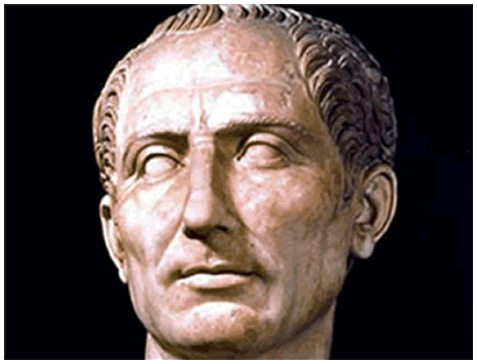
Modern Cryptography

Stefan Wolf

Department of Computer Science

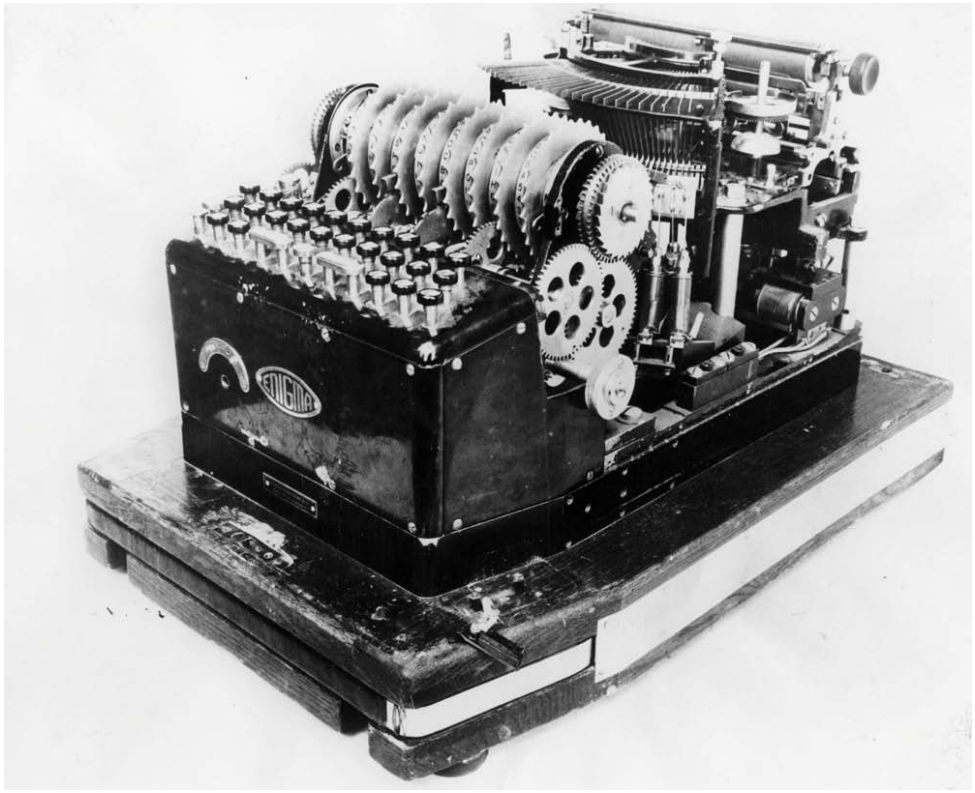
ETH Zürich



Caesar

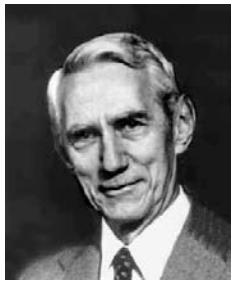
Problem: Key agreement

Arthur Scherbius



Bill Tutte

Alan Turing



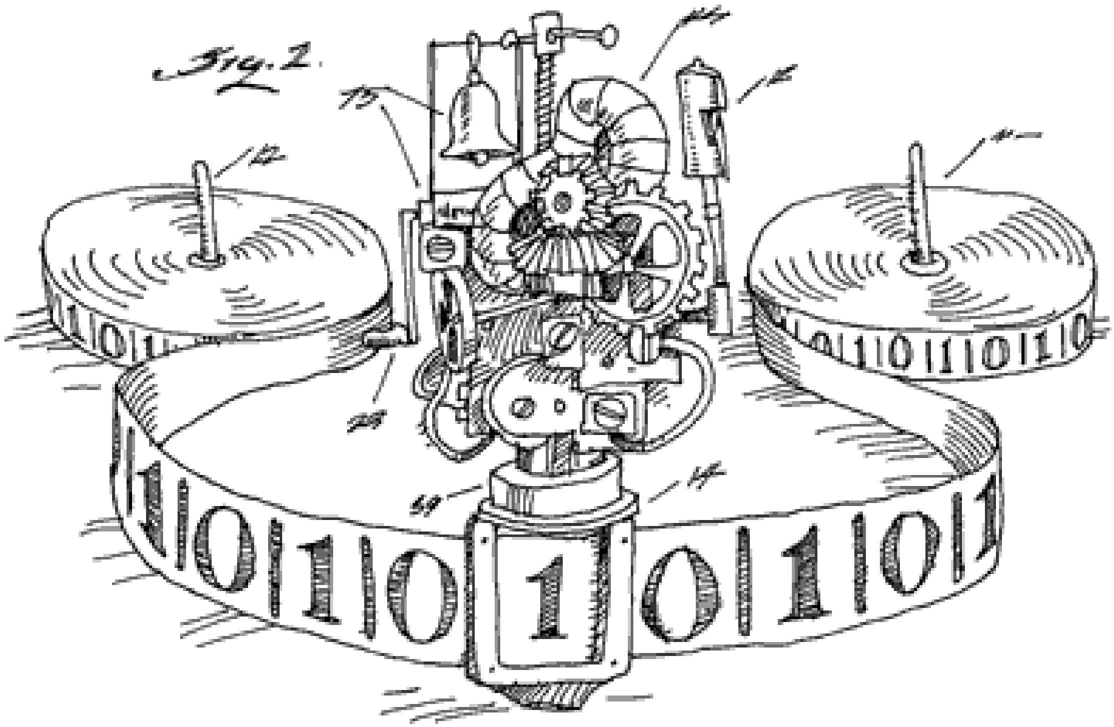
Claude Shannon

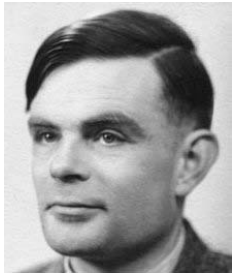
Bill Tutte

“At each step, you discarded the wheel position you felt in your bones was less likely. With reliable enough bones, you would end up with the entire key.”

⟶ Cryptography and cryptanalysis was “Voodoo magic.”

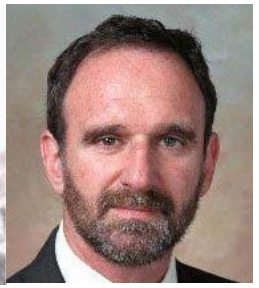
Alan Turing





Alan Turing

Whit Diffie



Martin Hellman

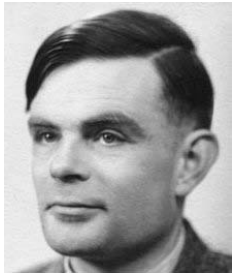
Breakthrough: "Public-Key Cryptography"

Advantage: No key agreement necessary

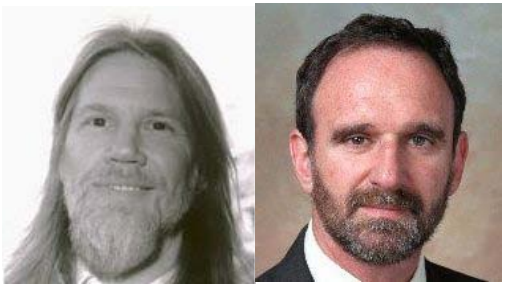
Disadvantage: Can be broken with sufficient computing power.

↓

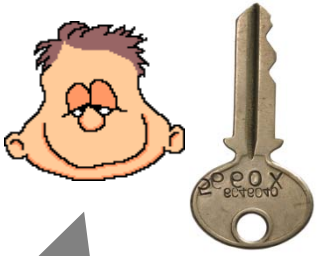
Today: with dramatic consequences for world economy.

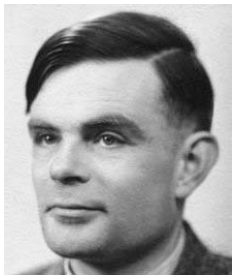


Alan Turing



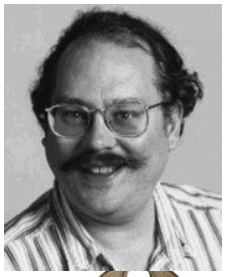
Whit Diffie **Martin Hellman**





Alan Turing

Ron Rivest Adi Shamir Len Adleman



Peter Shor

100294728364962[illegible]

[illegible]1?87309873838277

Quantum computer

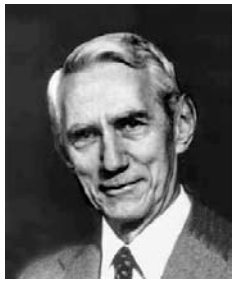
8297393892[illegible]3862199035391

Find  ?

1000000000000000000000000000000

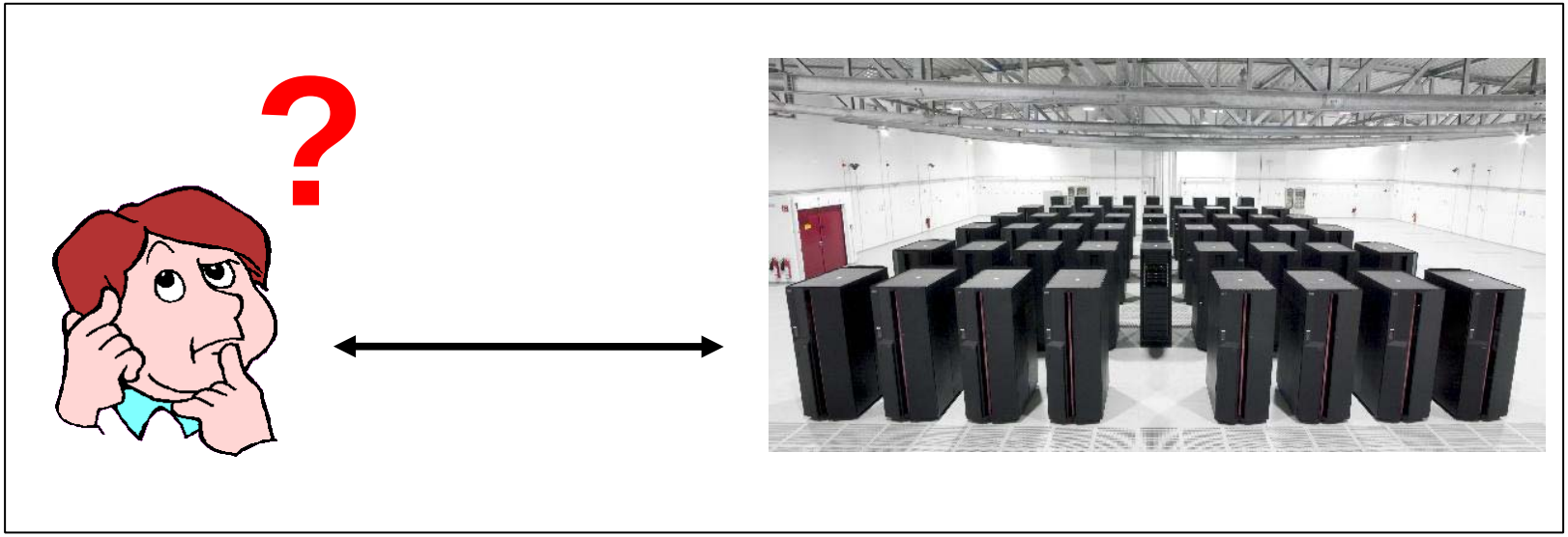
d prim[illegible]tor

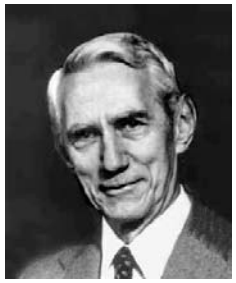
Times[illegible]niverse



Claude Shannon

Can security be based on lacking knowledge of the adversary?



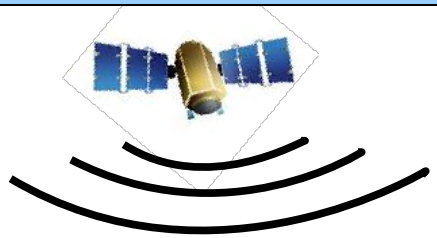


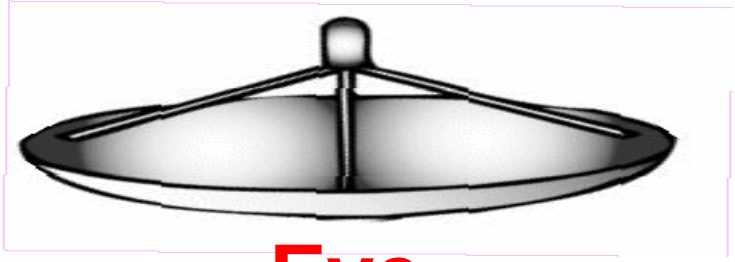
Claude Shannon

Ueli Maurer

Michael Rabin

Everlasting information-theoretic security

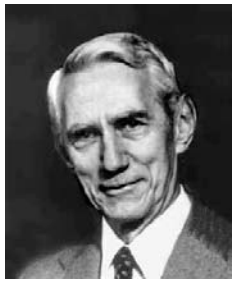




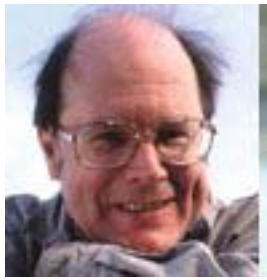
Eve

Alice

Bob



Claude Shannon



Charles Bennett

Gilles Brassard