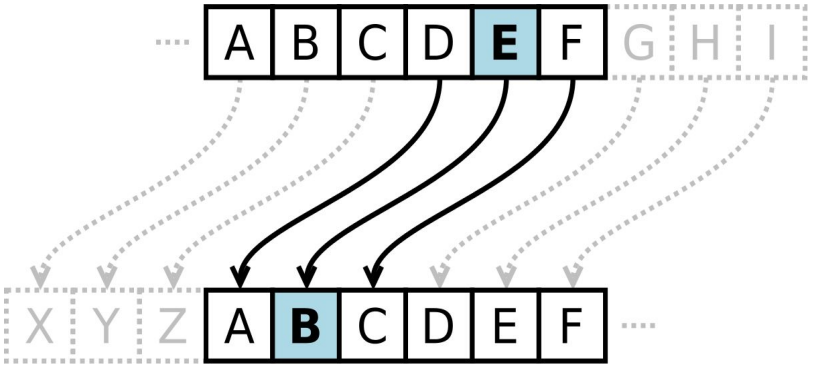
The History of Cryptography

March 15, 2018

Jack Dell, Peter Regas

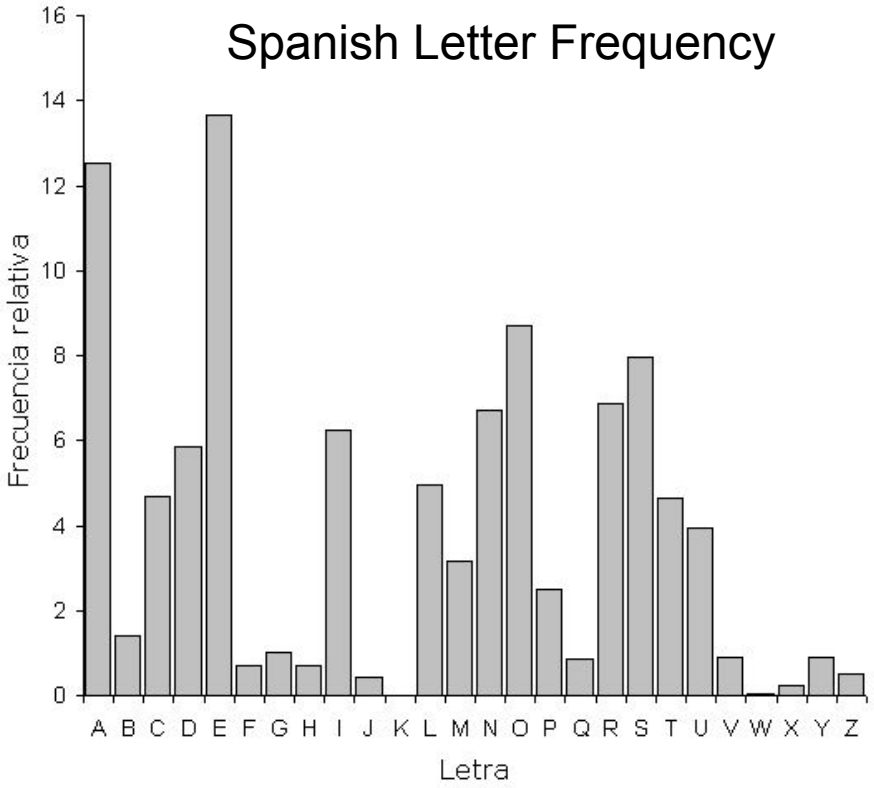
The Beginnings

Julius Caesar
Caesar Ciphers
50BC

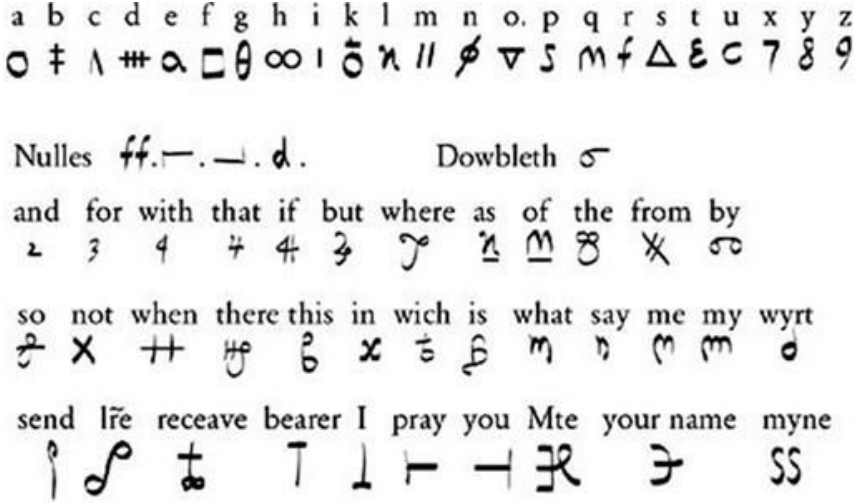


First form of Encryption Cracking

“Al-Kindi”
Arabic
Polymath
First discovered
Frequency Analysis
Method
850



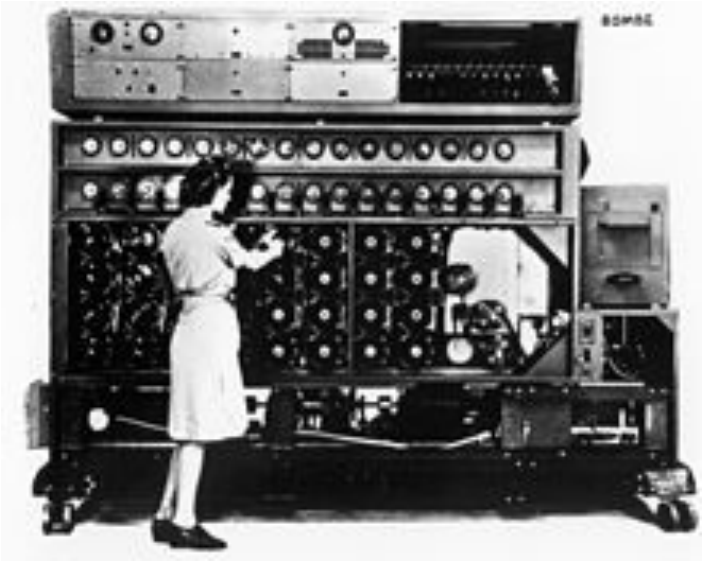
Combatting Frequency Analysis



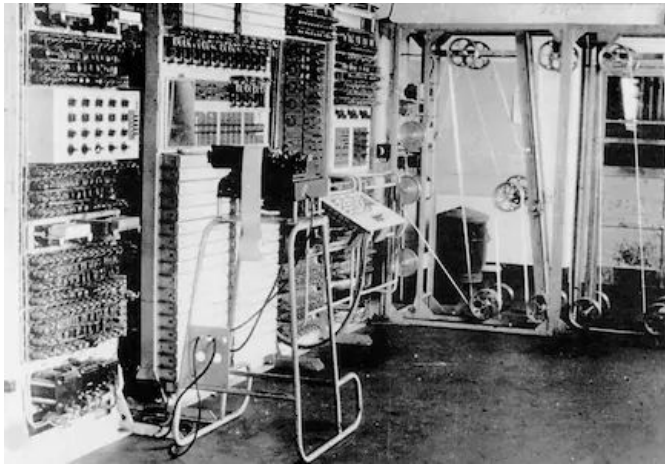
1. Still involved a basic cipher
2. Distribution and updating of nomenclators was challenging
3. Hard to have lots of people using same nomenclator

WWII

Bombe

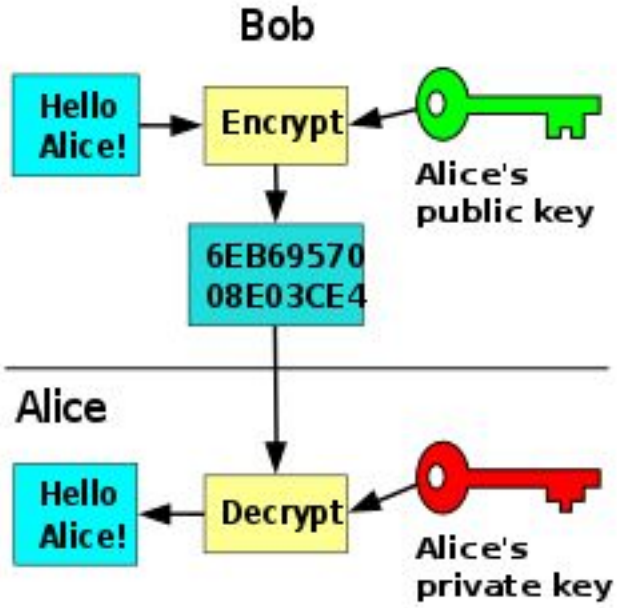


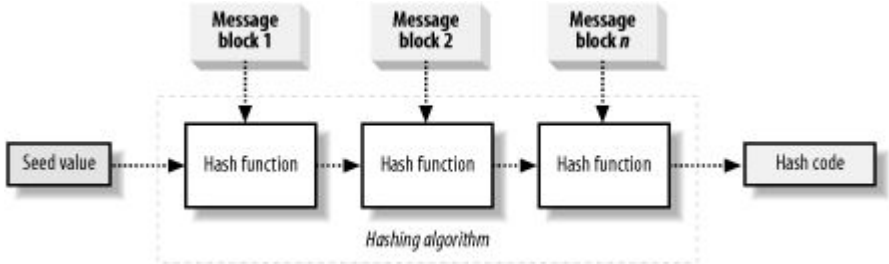
Colossus



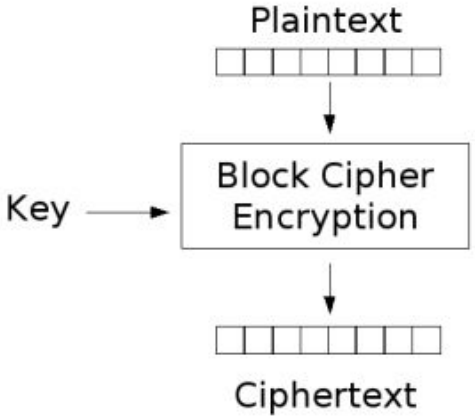
Public Keys

Solved the problem of encrypting two way communication

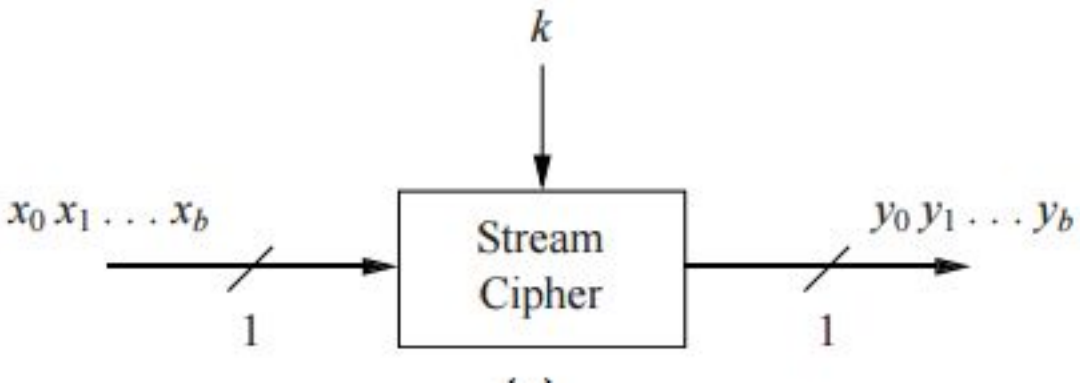




Stream & Block Ciphers

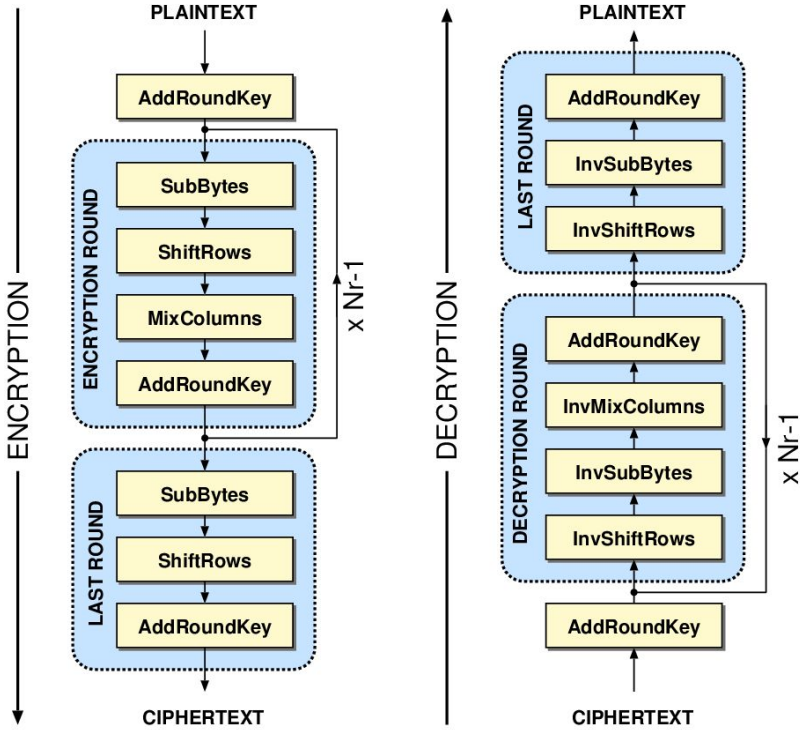


- Stream ciphers consist of long continuous data stream
- Data stream is plain text bits
- The bits are encoded using a cryptographic key and some chosen algorithm



- Block ciphers are very similar to stream ciphers
- Instead of individually encoding each bit, block ciphers will encode blocks of data of a specified size

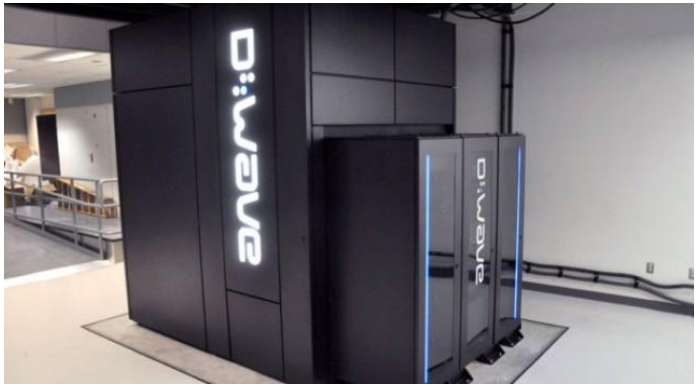
Modern Encryption Security

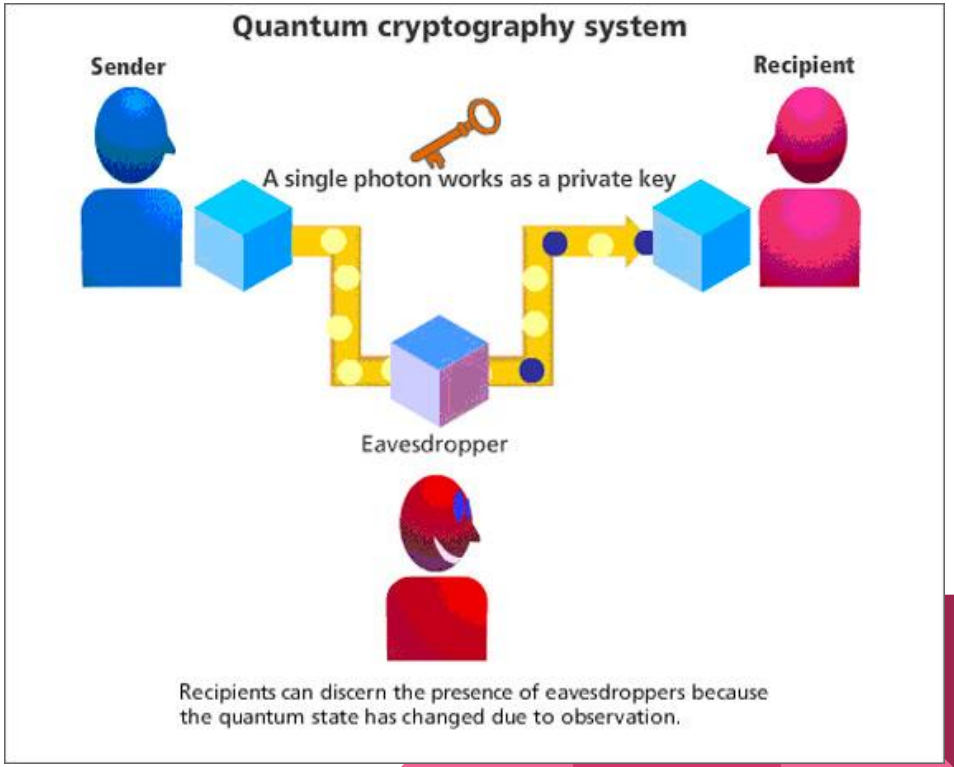


- Many modern Encryptions could be trivially decrypted with future advances
- Mathematics and computing technology is constantly advancing

Quantum Encryption

"Quantum cryptography makes use of the quantum-mechanical behavior of nature for the design and analysis of cryptographic schemes. Optimally (but not always), quantum cryptography allows for the design of cryptographic schemes whose security is guaranteed solely by the laws of nature" (Fehr, 2010, pg 494).





Conclusion

- Cryptography is a field the continues to reinvent itself over time.
- Is there a better solution with current technology?
- Is Quantum Cryptography the final step in this progression?