# Introduction to Cryptography

By Prof. R. Balasubramanian

Talk Given at IMSc
Mar 17, 2025

# What is Cryptography

Cryptology is the study and practice of techniques for secure communications in the presence of adversary.

It is derived from Greek words "*kryptos*" meaning hidden or secret and "*logia*" meaning study

Cryptology comprises of:

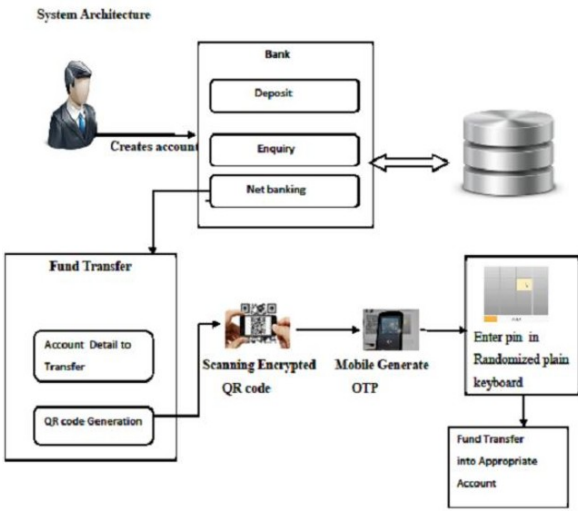
- Cryptography – Design of secure systems
- Cryptanalysis – Analyzing or breaking such systems

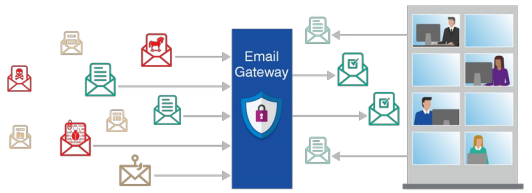
Is very ancient and has found mention in various scriptures.

Very important in defence, banking, governance, etc.

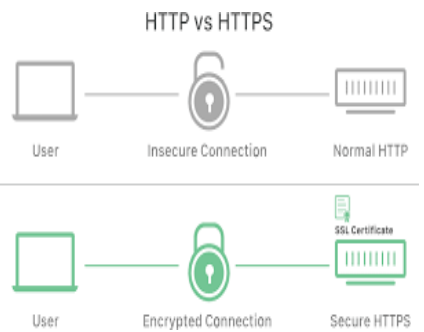
# Where is Crypto Used

- E-mail
- Accessing Websites
- Internet Services
- Open Source Social media
- Nextgen Telephony (5G)





# Enigma: WWII

- Electromechanical rotor device used by Germans for military communications
- Mariam Rejewski deduced detailed structure of Enigma to intercept German comminications
- Brought the war to an early conclusion

# Goals of Cryptography

Using cryptology, we hope to achieve

**Confidentiality** – No third party can read the data

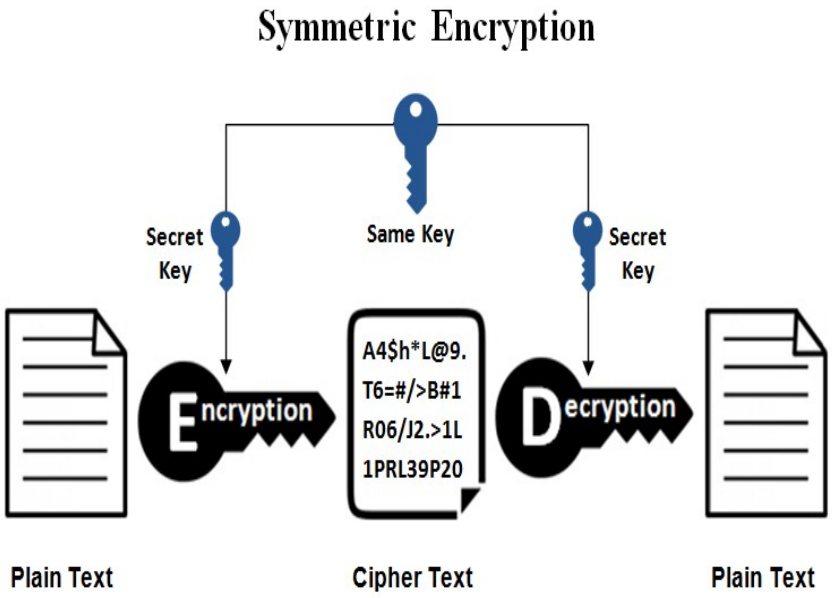
**Authentication** – The sender knows that the receiver knows a particular private key

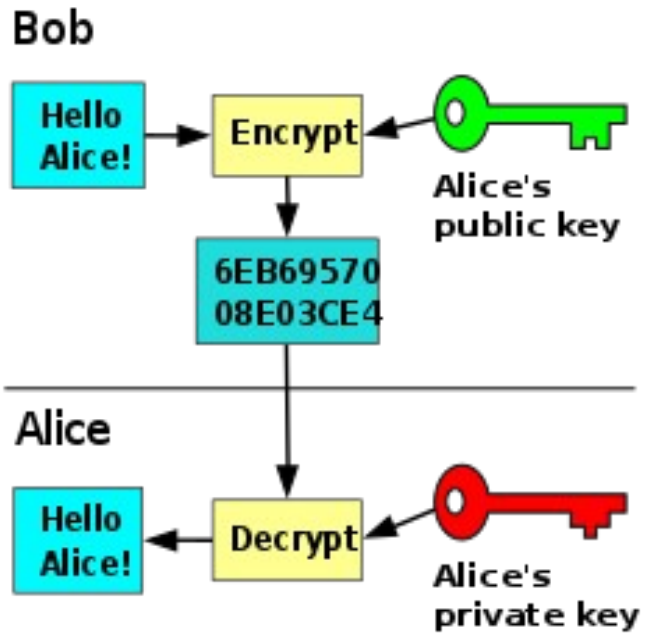
**Identification** – Binding between the private key and the individual

**Trust** – Third party certifies that a particular private key belongs to a particular individual

**Integrity** – Messages are not corrupted during transit

# Symmetric and Public Keys

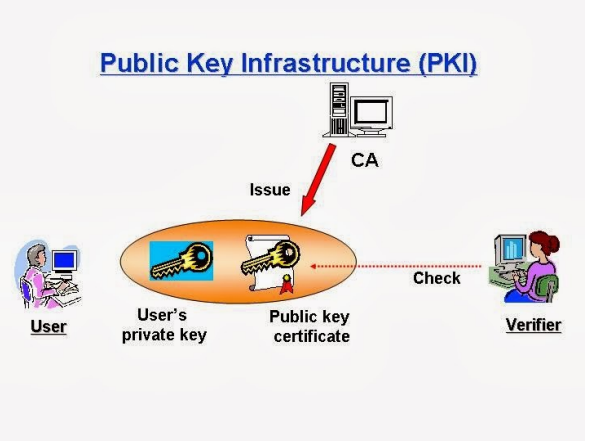


# Present Day Cryptosystems

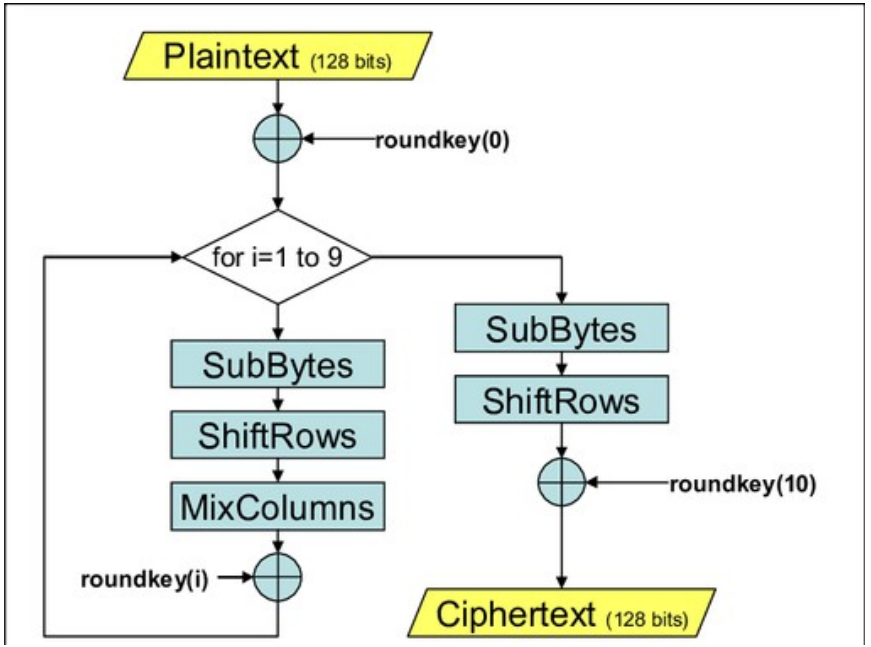
- RSA is a public key scheme
- Based on hardness of factoring integers
- Has wide range of applications: securely browsing webpages, internet banking, filing tax returns
- For building PKI: Infrastructure which binds entities with keys

| | |
|---|---|
| Key generation | $n = P * Q$<br>$d * e = 1 \bmod \Phi(n)$ |
| Encryption | $c = m^e \bmod n$<br>Public Key(n,e) |
| Decryption | $m = c^d \bmod n$<br>private key (d) |

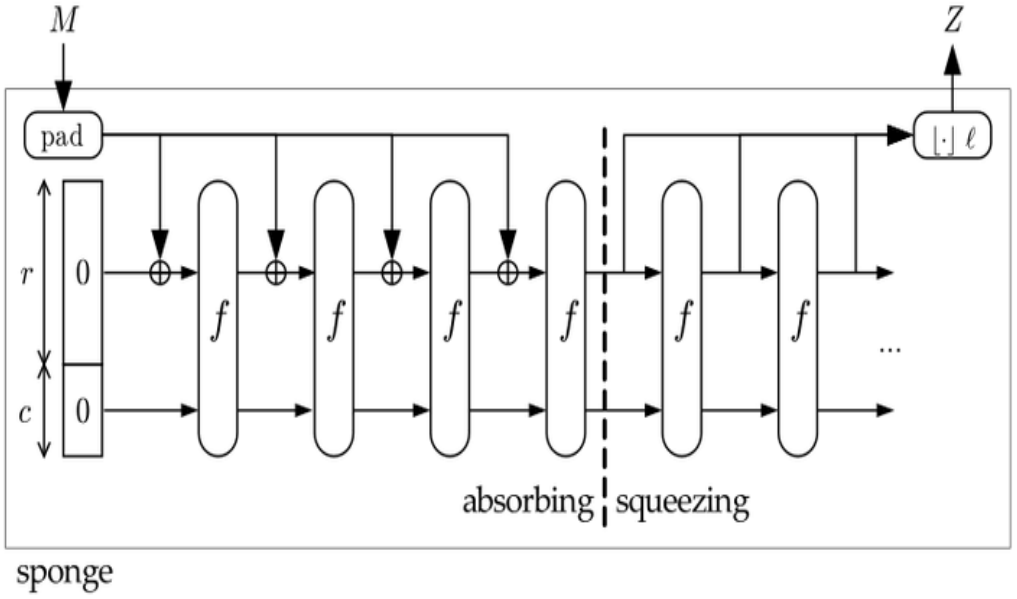


# Present Day Cryptosystems

AES is a block cipher which ensures data confidentiality

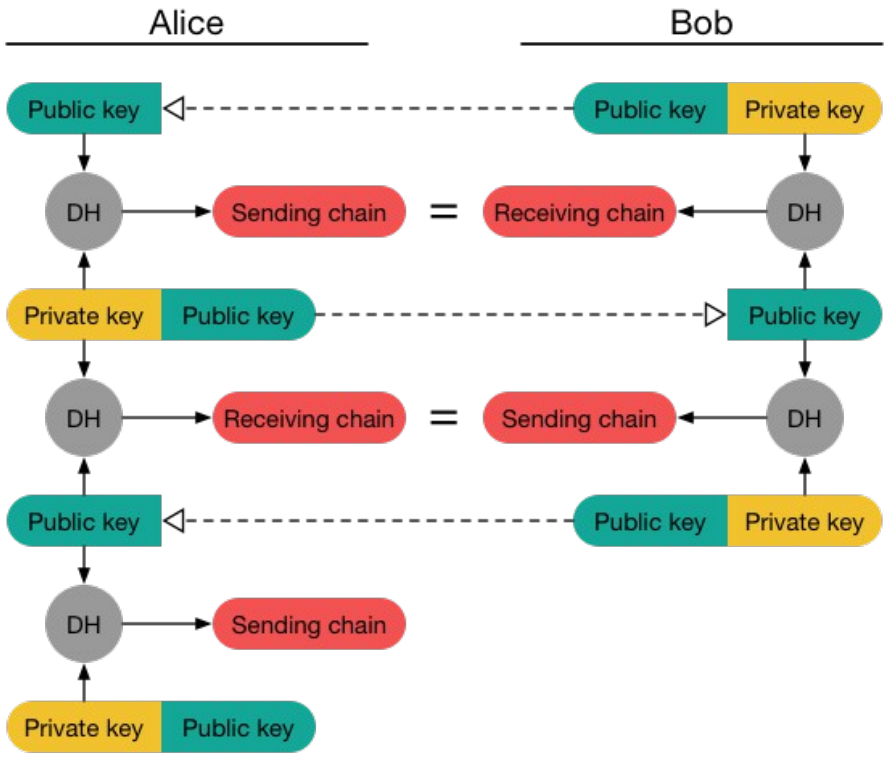



SHA-3 is a hash function that ensures data integrity



# Whatsapp and Signal

- Signal protocol designed by Open Whisper Systems
- End-to-end encryption is guaranteed
- Only sender and the recipient have the keys to unlock the message
- Strong key management and AES-256
- Some elliptic key cryptography is also involved for key management



# Authentication: Motivation for Uisng Digital Signatures

- Plays a very vital role in a Public Key Infrastructure
- Software updates, such that
  - any client can verify that the update is authentic
  - no malicious third party can fool a client into accepting a spurious update

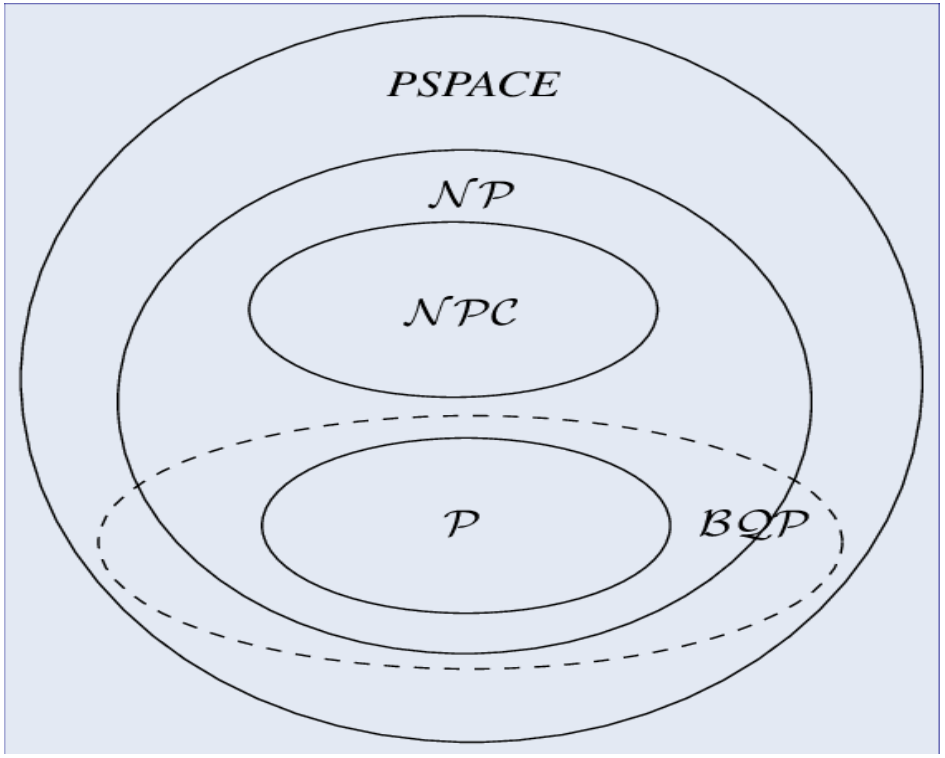
# Authentication: Motivation for Uisng Digital Signatures

- Generate a public key-secret key pair and distribute its public key to
- When releasing an update $m$, the company can compute a signature $\sigma$ using its secret key and send $(m, \sigma)$ to every client. The client verifies that $\sigma$ is a genuine signature on m using the company's public key. Accepts the update when the signature is genuine.

# How Will Quantum Computers Impact Security?

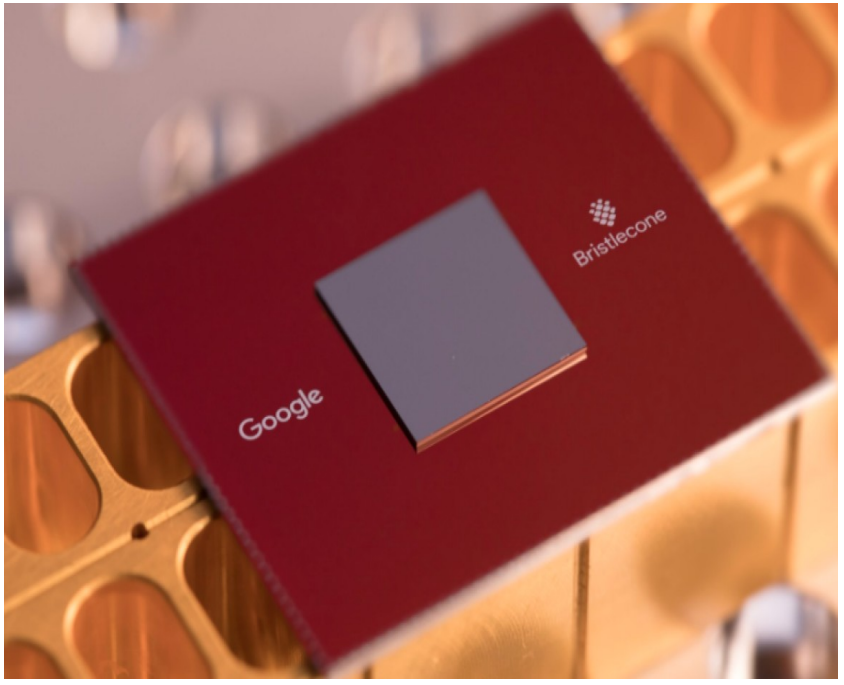
- Michele Mosca writes ``… national security and economic prosperity will be jeopardized as government, communications, transportation, banking, energy and other critical systems become vulnerable to hostile actions because our cryptography is no longer strong enough to protect us”
- Michele Mosca of U. Waterloo predicts 1/7 chance of breaking RSA-2048 by 2026 and 1/2 chance by 2031. This is based on rough estimate for designing fault tolerant scalable qubit
- In the near future, quantum computers without error correction will be able to approximately sample the output of random quantum circuits which state-of-the-art classical computers cannot simulate: arxiv 1608.00263

# Power of Quantum Computing

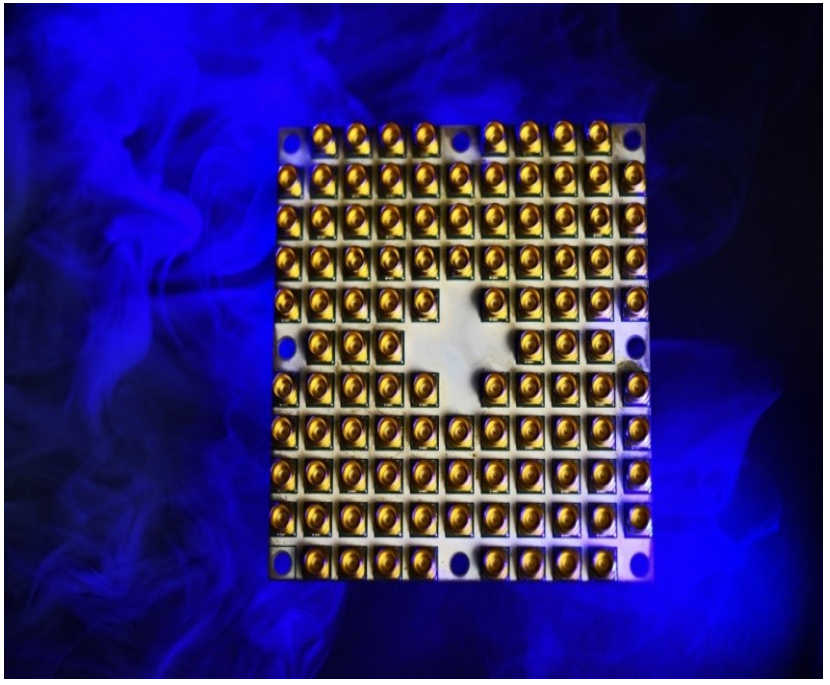



- Every efficient classical circuit can be efficiently implemented using quantum gates
- The class “Bounded Quantum Polynomial” includes class P
- It is believed that BQP lies somewhere between P and PSPACE

# Quantum Processors




**Google Bristlecone: 79 Qubits**



**Intel Tangle Lake: 49 Qubits**

# What Options Do We have?

- ✓ Stebila: "… expect the costs and challenges of using [qke] to decrease to the point where [such] systems can be deployed affordably and their behaviour can be certified."
- ➢ QKD plus symmetric key crypto is sufficient

- ✓ Use quantum resistant techniques to build crypto to run on classical computers: Quantum computers are good to solve only a few problems like factoring and DLP
- ➢ Use classical devices but different, quantum resistant crypto schemes

# Efforts for PQC Standardization

- There is a need to evolve new standards for public key cryptography
- New modules for internet protocols TLS, SSH; hardware like TPM, HSM
- ETSI PQC:

https://www.etsi.org/technologies/quantum-safe-cryptography

- NIST PQC:

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography