Quantum Computing and AppSec: Preparing for the Post-Quantum Threat

Quantum computing is advancing rapidly. Soon it will disrupt current encryption methods.

We'll explore real implications for application security and how to prepare now.

- Sheshananda Reddy Kandula

Thanks to the HOPE committee, volunteers, and everyone for organizing this excellent conference.

Whoami

@Sheshananda Reddy Kandula

15 years in Application Security/Cyber Security

Disclaimer

- The views and opinions expressed in this presentation are **my own**.
- They do not represent the views of my **employer** or any affiliated organization.
- This content reflects my **interest and learning** in quantum computing and application security.
- All work was prepared in my **own free time**.

Agenda

- Introduction
- Quantum Computing Basics
- Quantum Computing Threats
- Traditional Encryption Overview
- Cryptography in Application Security
- Attack Scenarios
- Mitigation Strategies
- Future Directions
- Q&A

You hear these words a lot in Next 40–45 min

Quantum Computing

Cryptography

Application Security

Post Quantum Cryptography

What is a Quantum Computer?

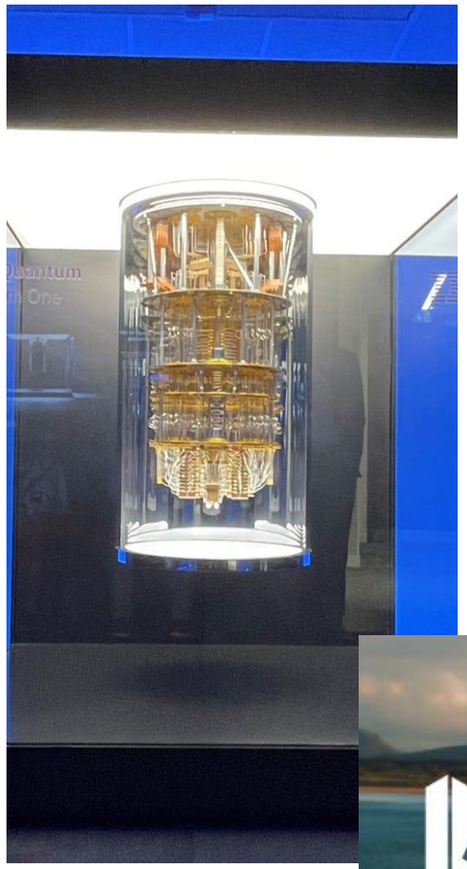
- Has anyone seen them?
- Online or in-person
- Touched physically?

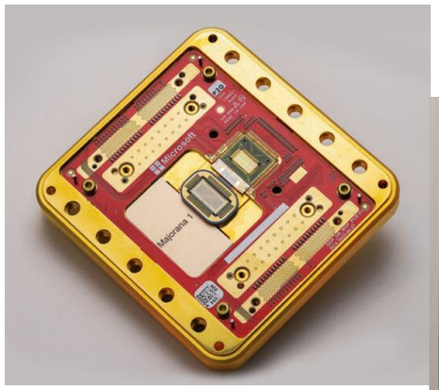
https://en.wikipedia.org/wiki/Chandelier#/media/File:Tatton_Park_2016_126.jpg
https://en.wikipedia.org/wiki/Chandelier#/media/File:Genoa_Le_Strade_Nuove_and_the_system_of_the_Palazzi_dei_Rolli-113860-trimmed.jpg

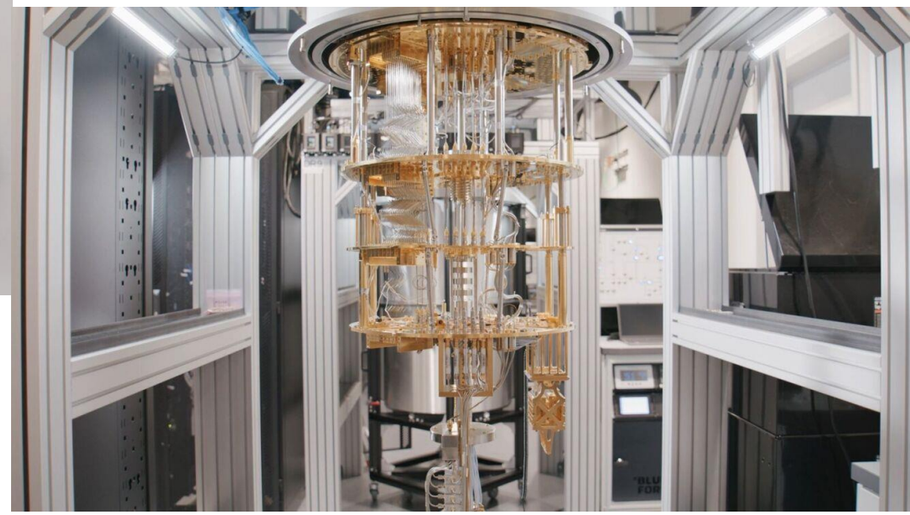
What is a Quantum Computer?

https://en.wikipedia.org/wiki/Chandelier#/media/File:Tatton_Park_2016_126.jpg
https://en.wikipedia.org/wiki/Chandelier#/media/File:Genoa_Le_Strade_Nuove_and_the_system_of_the_Palazzi_dei_Rolli-113860-trimmed.jpg

Quantum Computers in Real World







1. https://quantumai.google/quantumcomputer
2. https://research.ibm.com/blog/ibm-quantum-characterization-lab-tour
3. https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/
4. https://www.aboutamazon.com/news/aws/quantum-computing-aws-ocelot-chip
5. https://blog.google/technology/research/google-willow-quantum-chip/

Classical Computer Vs Quantum Computer

- A new kind of computer that uses the principles of **quantum mechanics** to process information.
- **Qubits** (quantum bits) instead of classical bits (0 or 1).
- **Quantum Computing**: that uses quantum mechanics principles to perform operations on data using qubits.

Understanding Quantum Bits

Classical Bits

Represent either 0 or 1

Can only be in one state at a time

Foundation of all modern computing

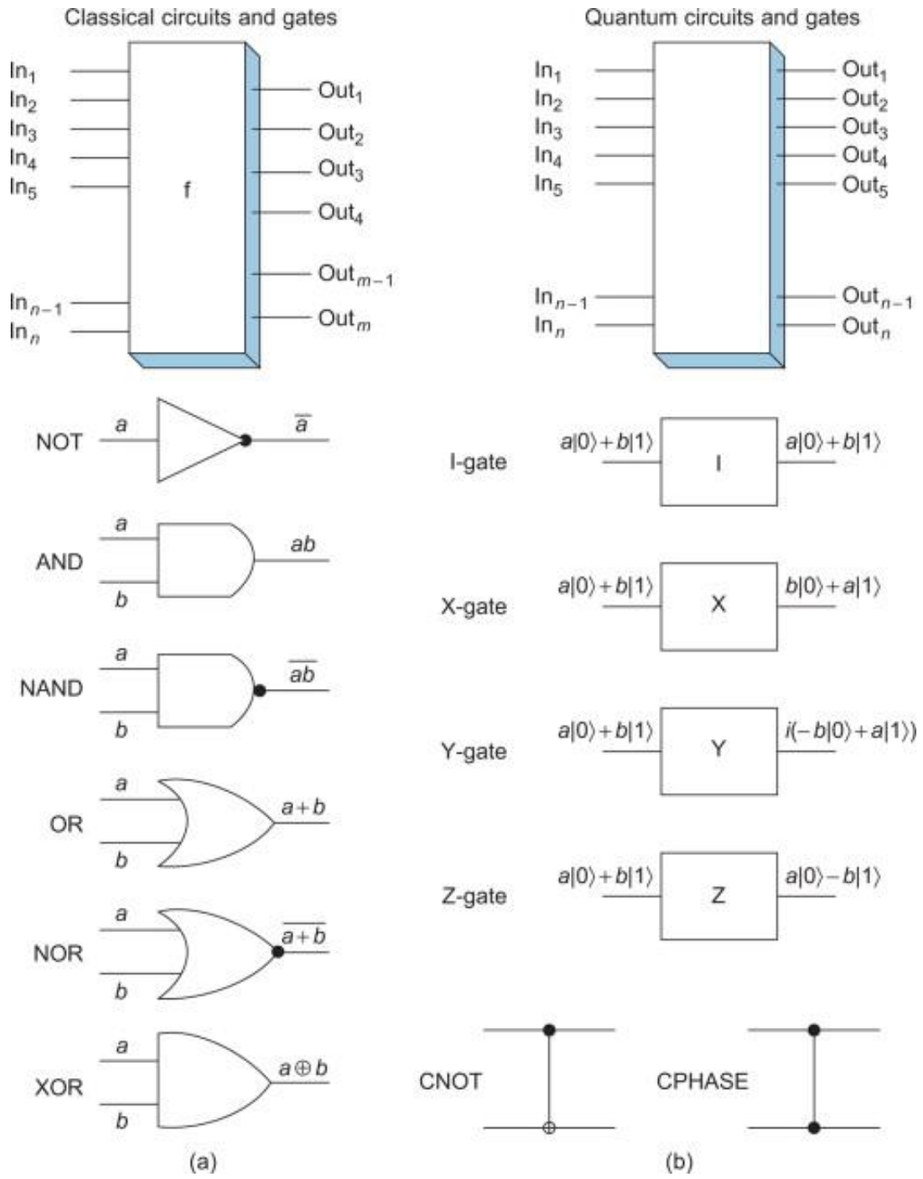
Quantum Bits (Qubits)

Can represent 0, 1, or both simultaneously

Exist in multiple states through superposition

Enable exponential computational power

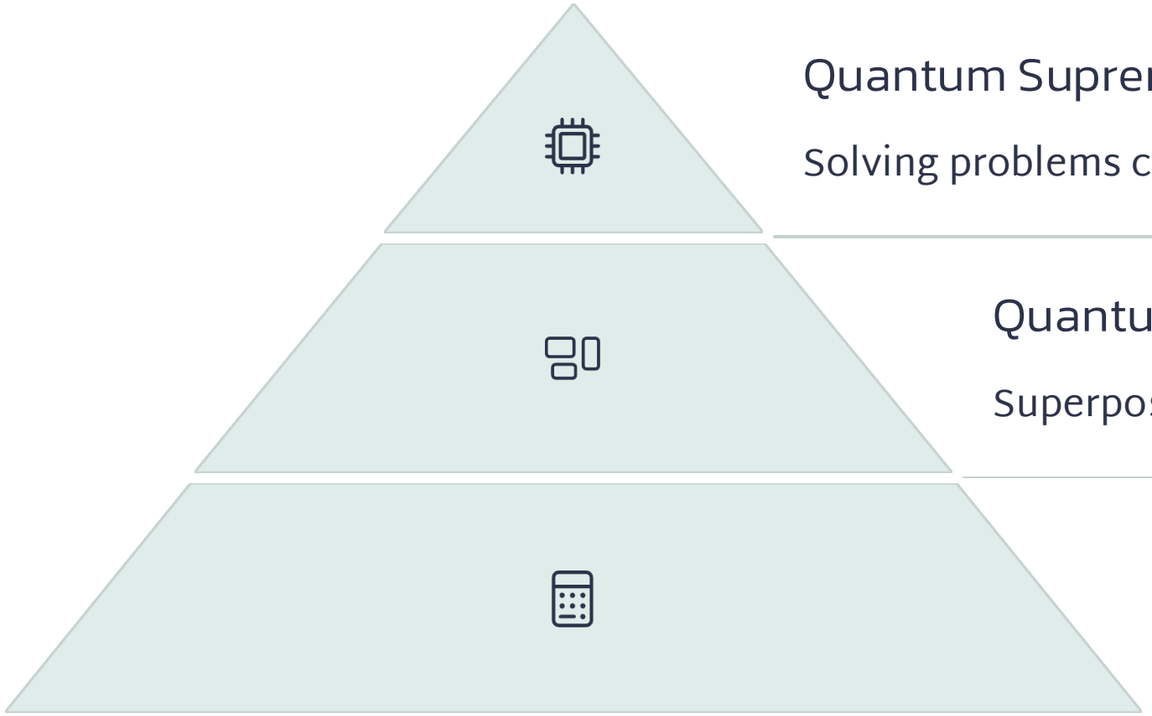
Classical Computer Vs Quantum Computer



https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.sciencedirect.com%2Ftopics%2Fcomputer-science%2Fclassical-computer&psig=AOvVaw3bmV-XVvD-3eHJhl6g4AJ6&ust=1755435954731000&source=images&cd=vfe&opi=89978449&ved=0CBYQjRxqFwoTCOCV2deyj48DFQAAAAAdAAAAABBH

Quantum Computing Advantages

Unlike classical bits, qubits operate on quantum mechanical principles. This enables exponential computational power.



Quantum Supremacy

Solving problems classical computers can't

Quantum Properties

Superposition, entanglement, and quantum tunneling

Quantum Bits

Qubits exist in multiple states simultaneously

Core Concepts

- **Superposition**: Particles exist in multiple states simultaneously.
- **Entanglement**: Two particles can be linked, affecting each other instantly, even across distances.

Quantum Superposition

Multiple States

Qubits exist in all possible states simultaneously

Probabilistic Nature

States exist with certain probabilities until measured

Measurement Impact

Observing a qubit collapses its state to either 0 or 1

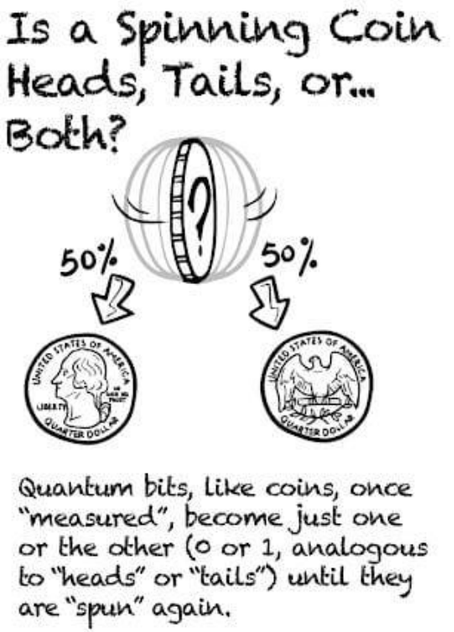
A coin spinning in the air is in a superposition of "heads" and "tails."

Why it Matters:

Allows quantum computers to perform computations on many possibilities concurrently.

Computational Power

Enables parallel computation of multiple possibilities



https://blogs.iu.edu/sciu/tag/parallelism/
https://www.nist.gov/image/superposition-quantum-computing-explainer

Quantum Entanglement

Connection

Qubits become linked regardless of distance

Correlation

Changes to one qubit instantly affect its partner

Speed

Information appears to transfer instantly

Applications

Enables secure communications and quantum teleportation

Quantum Computing Challenges

- **Error Correction**:
  - Maintaining quantum states against decoherence
- **Temperature**:
  - Operating at near absolute zero temperatures - Kelvin
- **Programming**:
  - Developing quantum algorithms and software

Quantum Computing Timeline

1980s
Theoretical foundations established by Feynman and Deutsch

1990s
Shor's algorithm proves quantum computers can factor large numbers

2010s
First quantum computers with 50+ qubits developed

2020s
Quantum advantage demonstrated for specific problems

Future
Commercial applications expected as technology matures

The Quantum Threat Timeline

Present Day

50-100 qubit systems with limited capabilities

3–5 Years

Error-corrected quantum computers emerge

5–10 Years

Cryptographically relevant quantum computers possible

10+ Years

Widespread quantum computing availability

Organizations should start planning their quantum migration strategy now. The "harvest now, decrypt later" threat is already active.

The Quantum Future

Research

Ongoing advancements in qubit stability and coherence

Industry

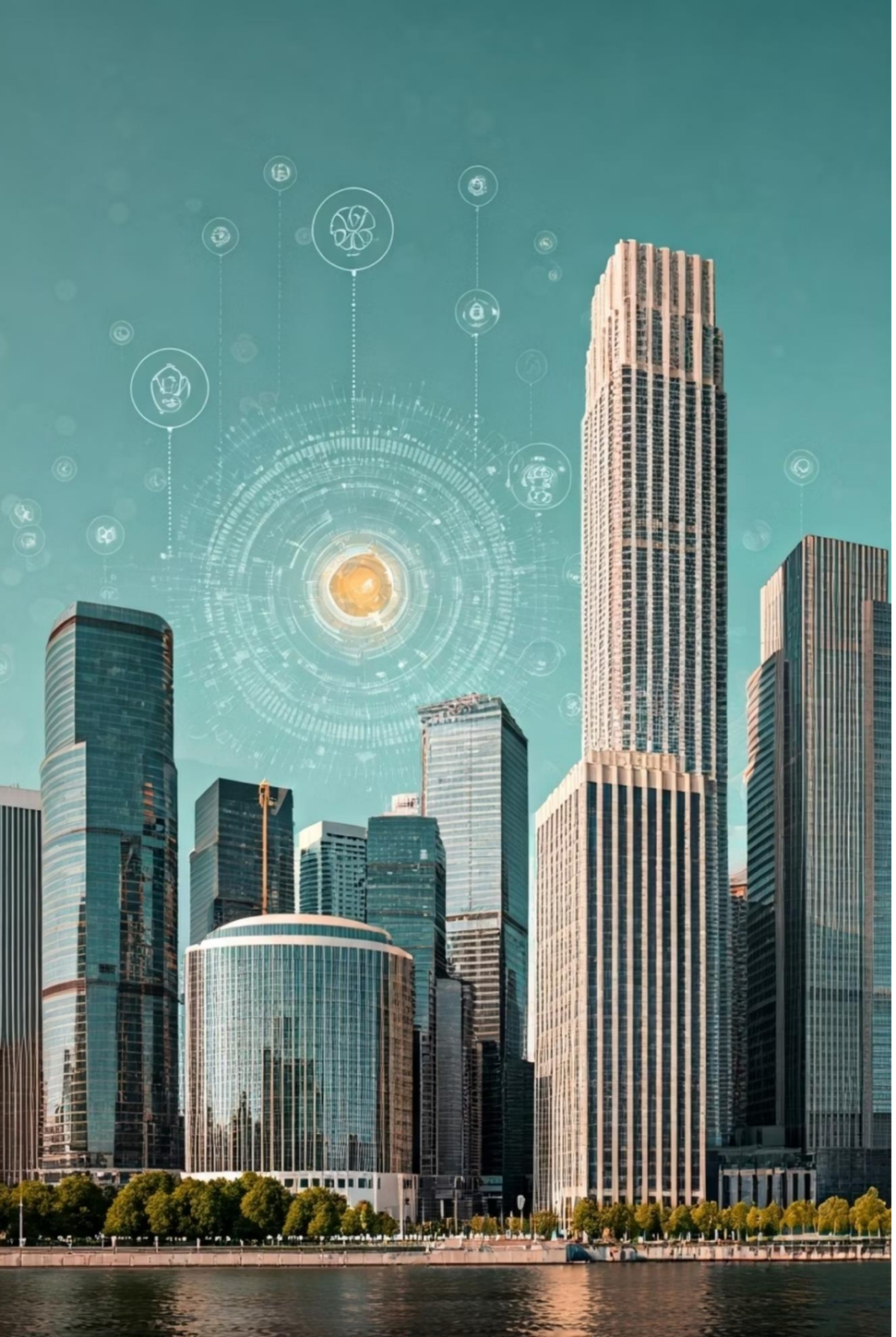
Growing investments from tech giants and startups

Applications

New solutions for previously unsolvable problems

Education

Expanding quantum computing curriculum worldwide



Quantum Computing Applications

Cryptography

- Breaking current encryption
- Creating unbreakable codes
- Secure communications

Scientific Research

- Molecular modeling
- Materials science
- Climate simulation

Optimization

- Supply chain logistics
- Financial modeling
- Traffic flow optimization

Examples of Potential

Demonstrating quantum superiority:

- **Quantum Simulation:**
  - **Purpose:** Simulating complex quantum systems (molecules, materials).
  - **Impact:** Revolutionary for drug discovery, materials science, and chemistry.
- **Quantum Machine Learning:**
  - **Purpose:** Enhancing AI tasks like pattern recognition and optimization.
  - **Impact:** Could lead to more powerful AI models.

Let’s move on to the **Cryptography** part

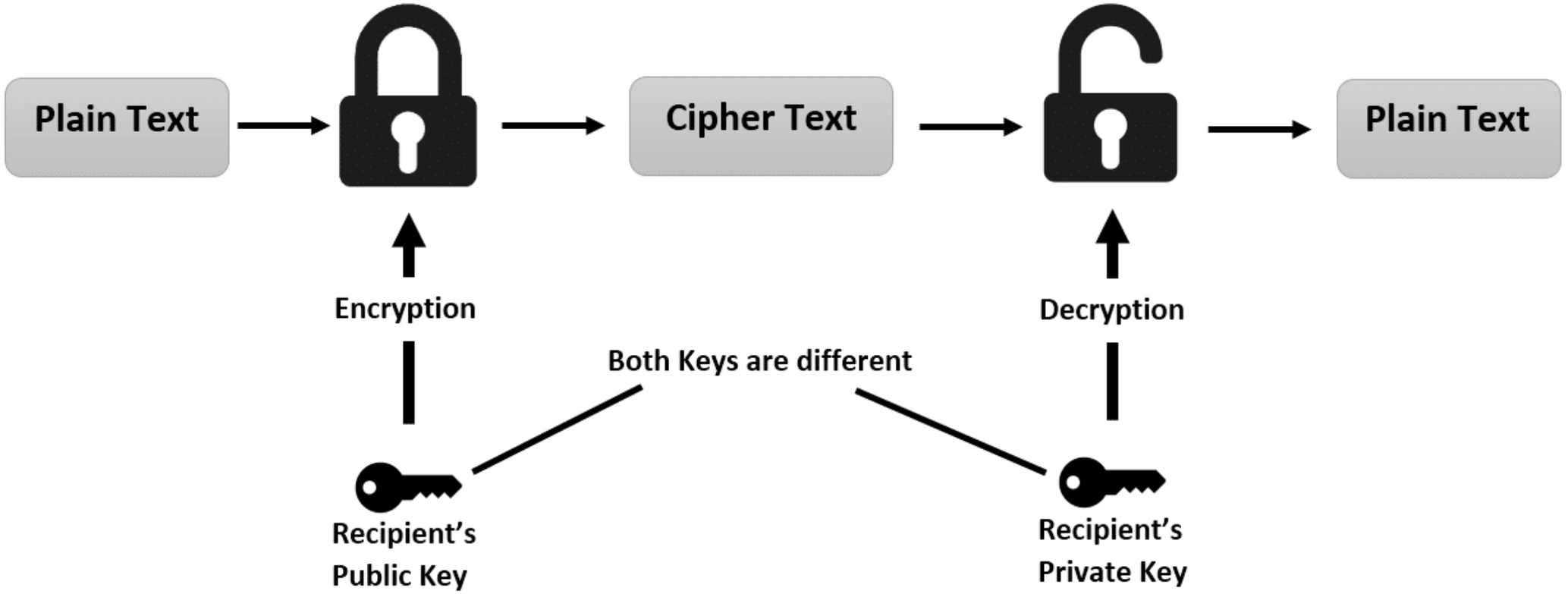
Encryption 101

- **Definition:** Encryption is the process of transforming information (plaintext) into an unreadable format (ciphertext) to protect its confidentiality.
- **Key Concepts:**
  - **Plaintext:** The original, readable data.
  - **Ciphertext:** The encrypted, unreadable data.
  - **Key:** A secret value used by an encryption algorithm.
  - **Encryption Algorithm:** A mathematical process for encryption and decryption.
  - **Decryption:** The process of converting ciphertext back into plaintext.
- **Importance:** Encryption is essential for protecting sensitive data in web applications, including passwords, user data, financial transactions, and more.
- **Types of Encryption:**
  - Symmetric Encryption
  - Asymmetric Encryption

Encryption Types

- **Symmetric Encryption:**
  - **Description:** Uses the same key for both encryption and decryption.
  - **Example:** AES (Advanced Encryption Standard)
  - **Advantages:** Fast and efficient.
  - **Disadvantages:** Key distribution can be complex and requires a secure channel.
- **Asymmetric Encryption:**
  - **Description:** Uses a pair of keys: a public key for encryption and a private key for decryption.
  - **Examples:** RSA (Rivest–Shamir–Adleman), ECC (Elliptic Curve Cryptography)
  - **Advantages:** Enables secure key exchange and digital signatures.
  - **Disadvantages:** Slower than symmetric encryption.
- **Encryption in Web Applications:**
  - **In Transit:** HTTPS/TLS encrypts data transmitted between web browsers and servers.
  - **At Rest:** Database encryption protects stored data; file encryption secures uploaded files.
  - **Hashing:** A one-way function used to store passwords securely.

Asymmetric Key Cryptography



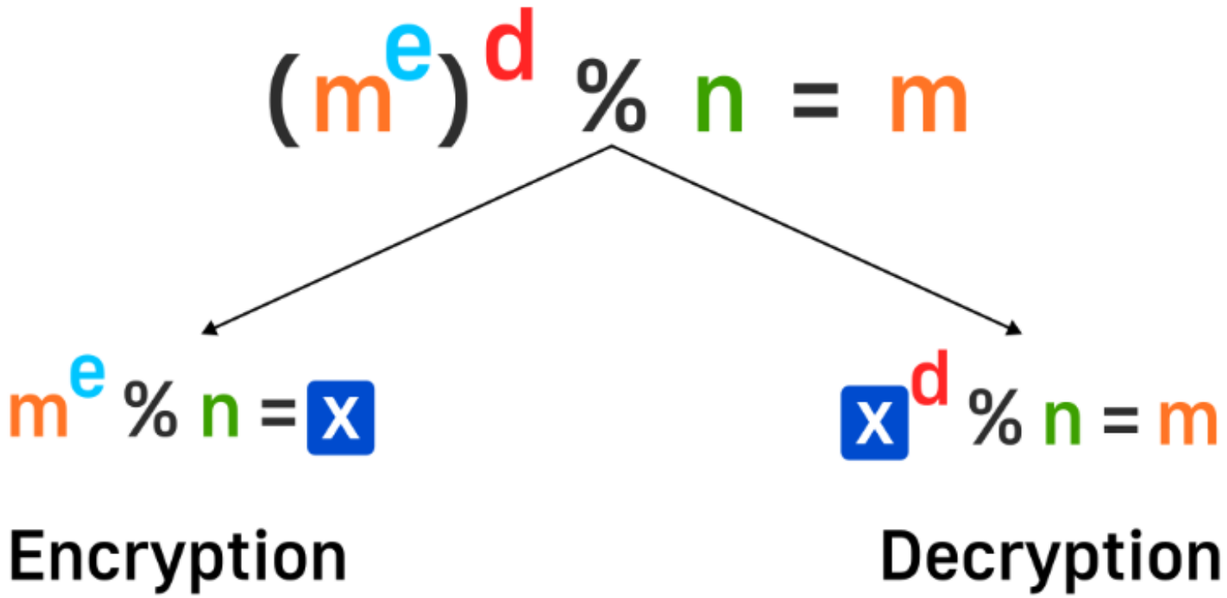
RSA, DSA, DH, ECC, etc.

https://user-images.githubusercontent.com/70335592/113505622-ba41f200-9548-11eb-8b52-5ab2ed3806f8.png

RSA Algorithm

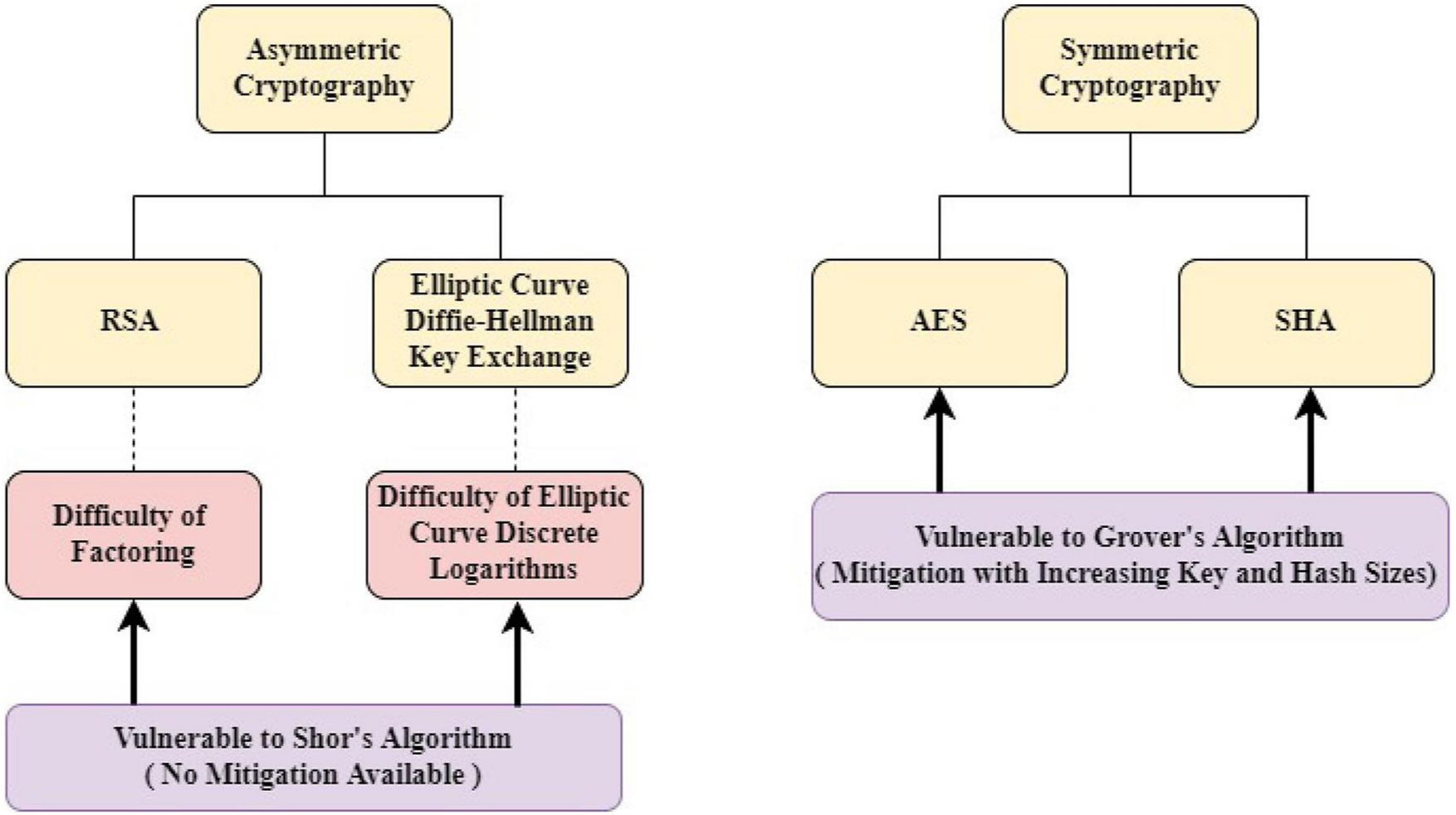
$$(m^e)^d \% n = m$$

```
m = message
e and n = public key
d = private key
n = modulus
```



https://hereket.com/posts/rsa-algorithm/

Cryptography Algorithms vs Post Quantum



https://www.sciencedirect.com/science/article/pii/S2590005622000777

Cryptography Algorithms vs Quantum Computers

Table 1. Impact of quantum computing on common cryptographic algorithms.

Cryptographic Algorithm	Type	Purpose	Impact from Large Scale Quantum Computer
AES	Symmetric Key	Encryption	Larger key sizes needed
SHA-2, SHA-3	—————	Hash Functions	Larger output needed
RSA	Public Key	Signatures, Key establishment	No longer secure
ECDSA, ECDH (Elliptical Curve Cryptography)	Public Key	Signatures, Key Exchange	No longer secure
DSA (Finite Field Cryptography)	Public Key	Signatures, Key Exchange	No longer secure

Most cryptocurrencies (Bitcoin, Ethereum, etc.) use **Elliptic Curve Cryptography (ECC)**, specifically **ECDSA** or **EdDSA**, for wallet and transaction security.

https://www.sciencedirect.com/science/article/pii/S2590005622000777

Quantum Computers can Break….

- SSL/TLS Traffic
- Certificates or PKI
- Blockchain or Crypto Currencies

Cryptography in Application Security

Cryptography forms a critical security layer for web and mobile applications. It protects data at rest, in transit, and in use.

The global cryptography market is projected to reach $8.4 billion by 2025. This growth reflects increasing concerns as 87% of organizations experienced application security breaches in 2024.

Cryptography Fundamentals in AppSec

Symmetric Encryption

Uses same key for encryption and decryption. Includes AES-256 and ChaCha20-Poly1305 algorithms.

Asymmetric Encryption

Uses key pairs for encryption and decryption. Provides foundation for digital signatures and secure key exchange.

RSA (Public Key Encryption)

ECC (Elliptic Curve Cryptography)

Hashing

One-way functions that create fixed-length output from variable input. Critical for password storage and data integrity.

Hashing Functions (SHA-256, SHA-3)

Key Management

The process of generating, storing, and rotating cryptographic keys. Often the weakest link in cryptographic implementations.

First Few Milli Seconds of HTTPS

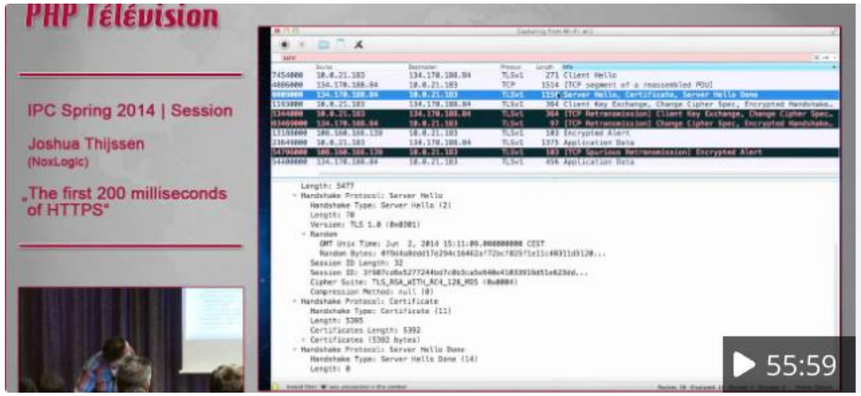
Information Security Stack Exchange

The First Few Milliseconds of an HTTPS Connection [TLS 1.2 / TLS_ECH...

In his blog post, 'The First Few Milliseconds of an HTTPS Connection', Jeff Moser does a wonderful job of walking through the TLS/SSL handshake process, and explaining...

[MIT CSAIL on Twitter / X]

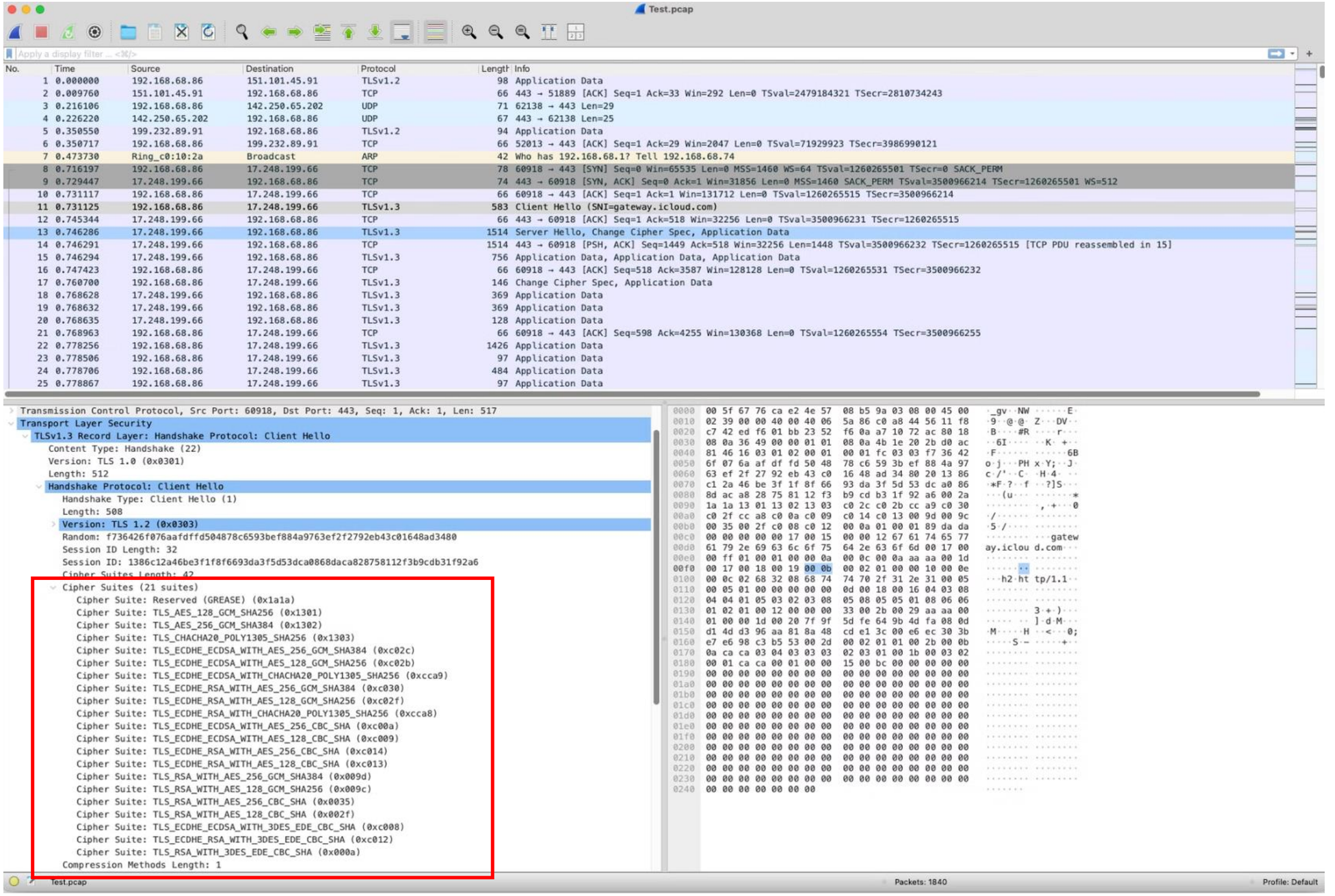
[The First Few Milliseconds of an HTTPS Connection]

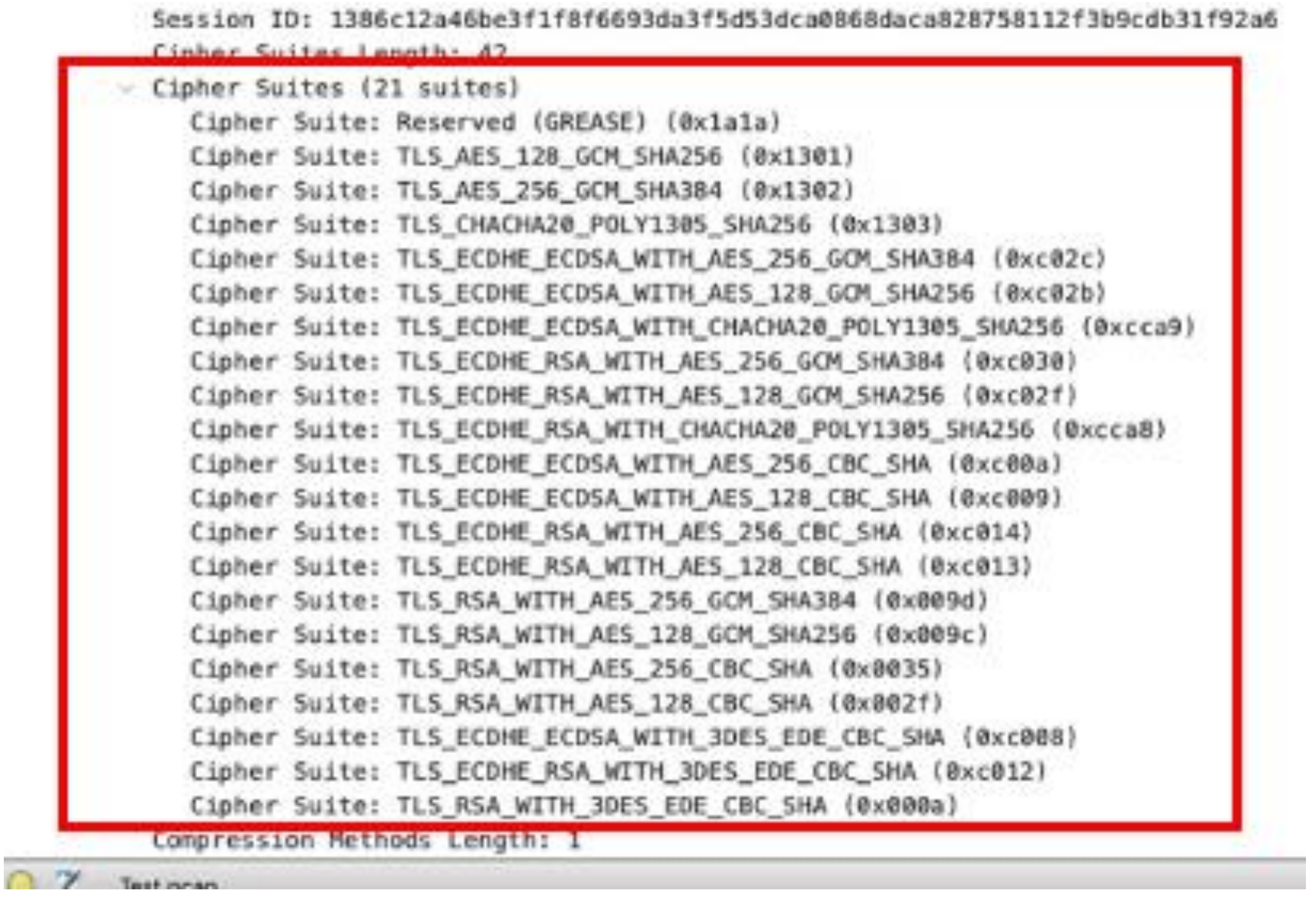


YouTube

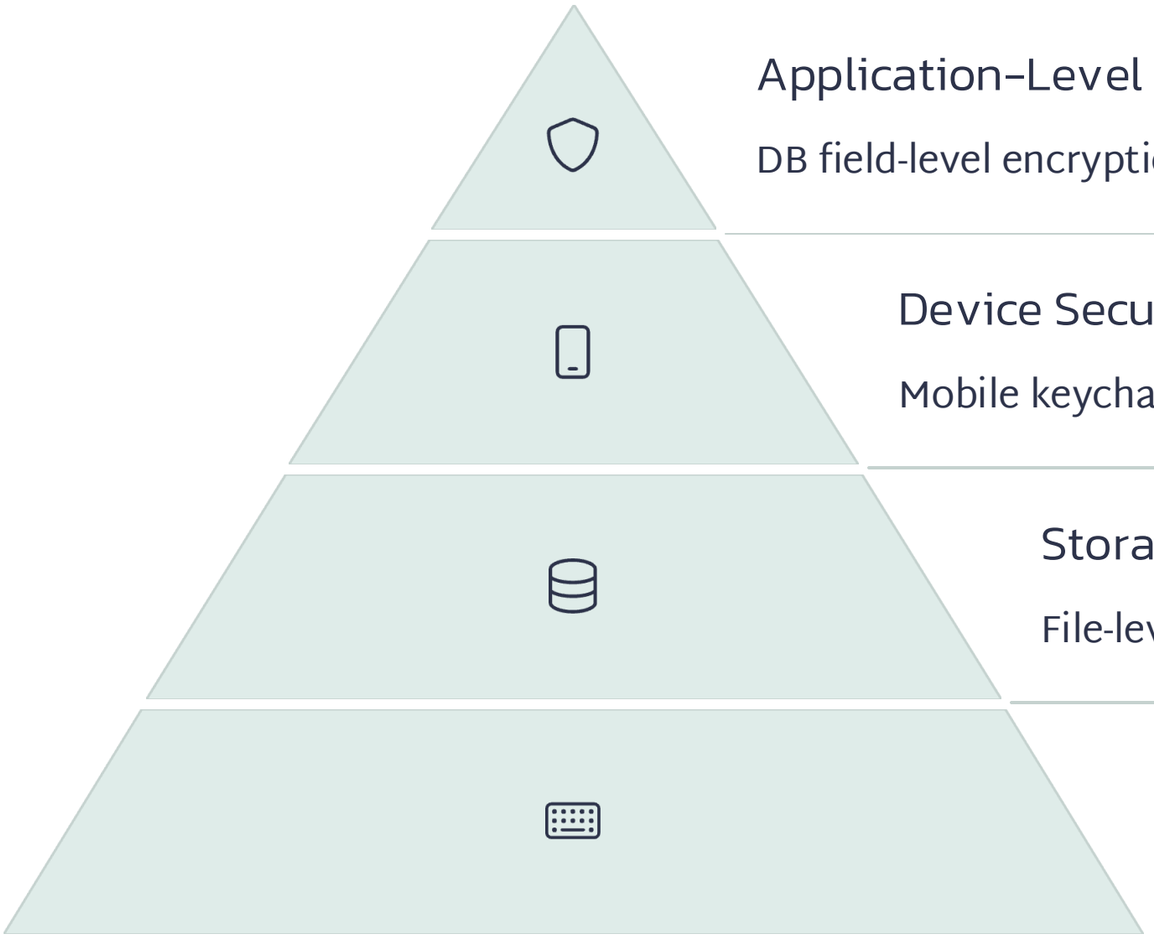
The first 200 milliseconds of HTTPS - Joshua Thijssen | IPC14

What happens when your browser connects to a HTTPS secure site? We all know it has to do something with certificates, blue and green address bars and sometimes...


Test.pcap
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.68.86 151.101.45.91 TLSv1.2 98 Application Data
2 0.009760 151.101.45.91 192.168.68.86 TCP 66 443 → 51889 [ACK] Seq=1 Ack=33 Win=292 Len=0 TSval=2479184321 TSecr=2810734243
3 0.216106 192.168.68.86 142.250.65.202 UDP 71 62138 → 443 Len=29
4 0.226220 142.250.65.202 192.168.68.86 UDP 67 443 → 62138 Len=25
5 0.350550 199.232.89.91 192.168.68.86 TLSv1.2 94 Application Data
6 0.350717 192.168.68.86 199.232.89.91 TCP 66 52013 → 443 [ACK] Seq=1 Ack=29 Win=2047 Len=0 TSval=71929923 TSecr=3986990121
7 0.473730 Ring_c0:10:2a Broadcast ARP 42 Who has 192.168.68.1? Tell 192.168.68.74
8 0.716197 192.168.68.86 17.248.199.66 TCP 78 60918 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1260265501 TSecr=0 SACK_PERM
9 0.729447 17.248.199.66 192.168.68.86 TCP 74 443 → 60918 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM TSval=3500966214 TSecr=1260265501 WS=512
10 0.731117 192.168.68.86 17.248.199.66 TCP 66 60918 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=1260265515 TSecr=3500966214
11 0.731125 192.168.68.86 17.248.199.66 TLSv1.3 583 Client Hello (SNI=gateway.icloud.com)
12 0.745344 17.248.199.66 192.168.68.86 TCP 66 443 → 60918 [ACK] Seq=1 Ack=518 Win=32256 Len=0 TSval=3500966231 TSecr=1260265515
13 0.746286 17.248.199.66 192.168.68.86 TLSv1.3 1514 Server Hello, Change Cipher Spec, Application Data
14 0.746291 17.248.199.66 192.168.68.86 TCP 1514 443 → 60918 [PSH, ACK] Seq=1449 Ack=518 Win=32256 Len=1448 TSval=3500966232 TSecr=1260265515 [TCP PDU reassembled in 15]
15 0.746294 17.248.199.66 192.168.68.86 TLSv1.3 756 Application Data, Application Data, Application Data
16 0.747423 192.168.68.86 17.248.199.66 TCP 66 60918 → 443 [ACK] Seq=518 Ack=3587 Win=128128 Len=0 TSval=1260265531 TSecr=3500966232
17 0.760700 192.168.68.86 17.248.199.66 TLSv1.3 146 Change Cipher Spec, Application Data
18 0.768628 17.248.199.66 192.168.68.86 TLSv1.3 369 Application Data
19 0.768632 17.248.199.66 192.168.68.86 TLSv1.3 369 Application Data
20 0.768635 17.248.199.66 192.168.68.86 TLSv1.3 128 Application Data
21 0.768963 192.168.68.86 17.248.199.66 TCP 66 60918 → 443 [ACK] Seq=598 Ack=4255 Win=130368 Len=0 TSval=1260265554 TSecr=3500966255
22 0.778256 192.168.68.86 17.248.199.66 TLSv1.3 1426 Application Data
23 0.778506 192.168.68.86 17.248.199.66 TLSv1.3 97 Application Data
24 0.778706 192.168.68.86 17.248.199.66 TLSv1.3 484 Application Data
25 0.778867 192.168.68.86 17.248.199.66 TLSv1.3 97 Application Data
Transmission Control Protocol, Src Port: 60918, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: f736426f076aafdffd504878c6593bef884a9763ef2f2792eb43c01648ad3480
Session ID Length: 32
Session ID: 1386c12a46be3f1f8f6693da3f5d53dca0868daca828758112f3b9cdb31f92a6
Cipher Suites Length: 42
Cipher Suites (21 suites)
Cipher Suite: Reserved (GREASE) (0x1a1a)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
Cipher Suite: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Compression Methods Length: 1
0000 00 5f 67 76 ca e2 4e 57 08 b5 9a 03 08 00 45 00 ._gv..NW ......E.
0010 02 39 00 00 40 00 40 06 5a 86 c0 a8 44 56 11 f8 .9..@.@. Z...DV..
0020 c7 42 ed f6 01 bb 23 52 f6 0a a7 10 72 ac 80 18 .B....#R ....r...
0030 08 0a 36 49 00 00 01 01 08 0a 4b 1e 20 2b d0 ac ..6I.... ..K. +..
0040 81 46 16 03 01 02 00 01 00 01 fc 03 03 f7 36 42 .F...... ......6B
0050 6f 07 6a af df fd 50 48 78 c6 59 3b ef 88 4a 97 o.j...PH x.Y;..J.
0060 63 ef 2f 27 92 eb 43 c0 16 48 ad 34 80 20 13 86 c./'..C. .H.4. ..
0070 c1 2a 46 be 3f 1f 8f 66 93 da 3f 5d 53 dc a0 86 .*F.?..f ..?]S...
0080 8d ac a8 28 75 81 12 f3 b9 cd b3 1f 92 a6 00 2a ...(u... ....*
0090 1a 1a 13 01 13 02 13 03 c0 2c c0 2b cc a9 c0 30 ....,.+...0
00a0 c0 2f cc a8 c0 0a c0 09 c0 14 c0 13 00 9d 00 9c ./...... ....
00b0 00 35 00 2f c0 08 c0 12 00 0a 01 00 01 89 da da .5./.... ....
00c0 00 00 00 00 00 17 00 15 00 00 12 67 61 74 65 77 ....gatew
00d0 61 79 2e 69 63 6c 6f 75 64 2e 63 6f 6d 00 17 00 ay.iclou d.com...
00e0 00 ff 01 00 01 00 00 0a 00 0c 00 0a aa aa 00 1d ....
00f0 00 17 00 18 00 19 00 0b 00 02 01 00 00 10 00 0e ....
0100 00 0c 02 68 32 08 68 74 74 70 2f 31 2e 31 00 05 ...h2.ht tp/1.1..
0110 00 05 01 00 00 00 00 00 0d 00 18 00 16 04 03 08 ....
0120 04 04 01 05 03 02 03 08 05 08 05 05 01 08 06 06 ....
0130 01 02 01 00 12 00 00 00 33 00 2b 00 29 aa aa 00 .... 3.+.)...
0140 01 00 00 1d 00 20 7f 9f 5d fe 64 9b 4d fa 08 0d ....].d.M...
0150 d1 4d d3 96 aa 81 8a 48 cd e1 3c 00 e6 ec 30 3b .M.....H ..<...0;
0160 e7 e6 98 c3 b5 53 00 2d 00 02 01 01 00 2b 00 0b .....S.- .....+..
0170 0a ca ca 03 04 03 03 03 02 03 01 00 1b 00 03 02 ....
0180 00 01 ca ca 00 01 00 00 15 00 bc 00 00 00 00 00 ....
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0240 00 00 00 00 00 00 00 00 ....
Test.pcap
Packets: 1840
Profile: Default


Session ID: 1386c12a46be3f1f8f6693da3f5d53dca0868daca828758112f3b9cdb31f92a6
Cipher Suites Length: 42
Cipher Suites (21 suites)
Cipher Suite: Reserved (GREASE) (0x1a1a)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
Cipher Suite: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Compression Methods Length: 1

Data-at-Rest Protection



Application-Level Encryption

DB field-level encryption for sensitive web app data

Device Security

Mobile keychain/keystore with hardware-backed encryption

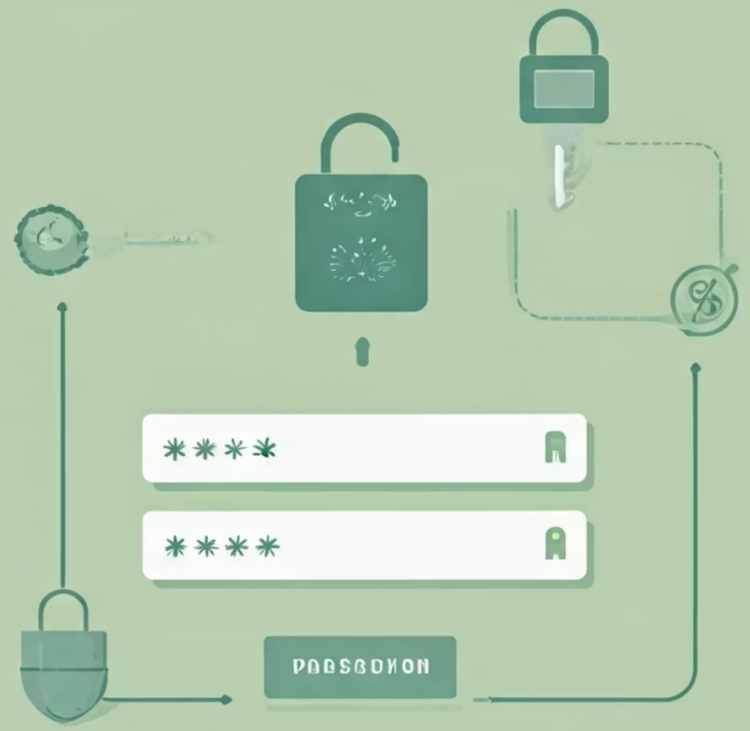
Storage Encryption

File-level and full disk encryption strategies

Key Derivation

Encryption keys derived from user authentication

Proper data-at-rest protection requires multiple layers of security working together.



Authentication Cryptography

Password Hashing

- PBKDF2: Widely supported
- bcrypt: Adaptive work factor
- Argon2: Memory-hard function

Token-Based Auth

- JWT: JSON Web Tokens
- PASETO: Platform-Agnostic Security Tokens
- FIDO2: Passwordless authentication

Multi-Factor Authentication

- TOTP: Time-based One-Time Passwords
- Hardware security keys
- Biometrics with secure enclaves

Mobile App-Specific Cryptography

Android Keystore

Hardware-backed secure key storage system for Android applications

iOS Secure Enclave

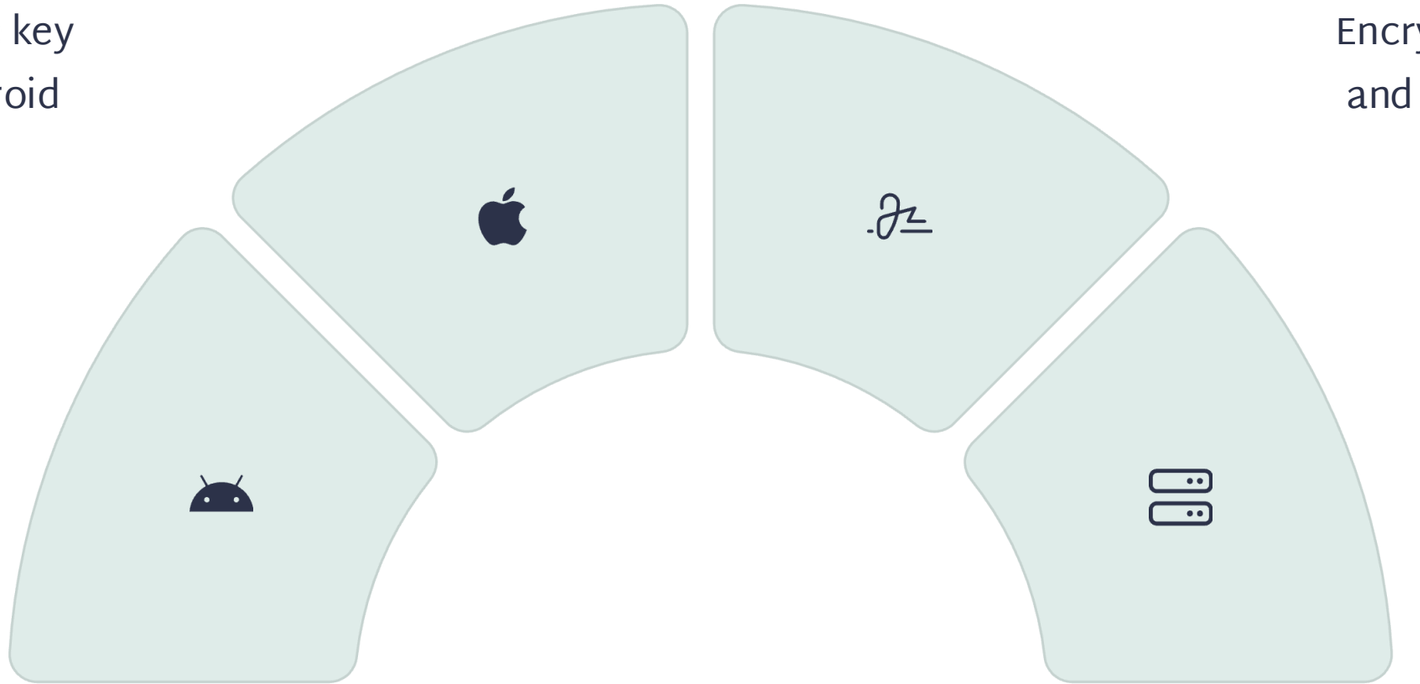
Dedicated security processor that isolates sensitive cryptographic operations

Code Signing

Verifies app integrity and authenticity through cryptographic signatures

Secure Storage

Encrypted SQLite databases and secure file systems for local data



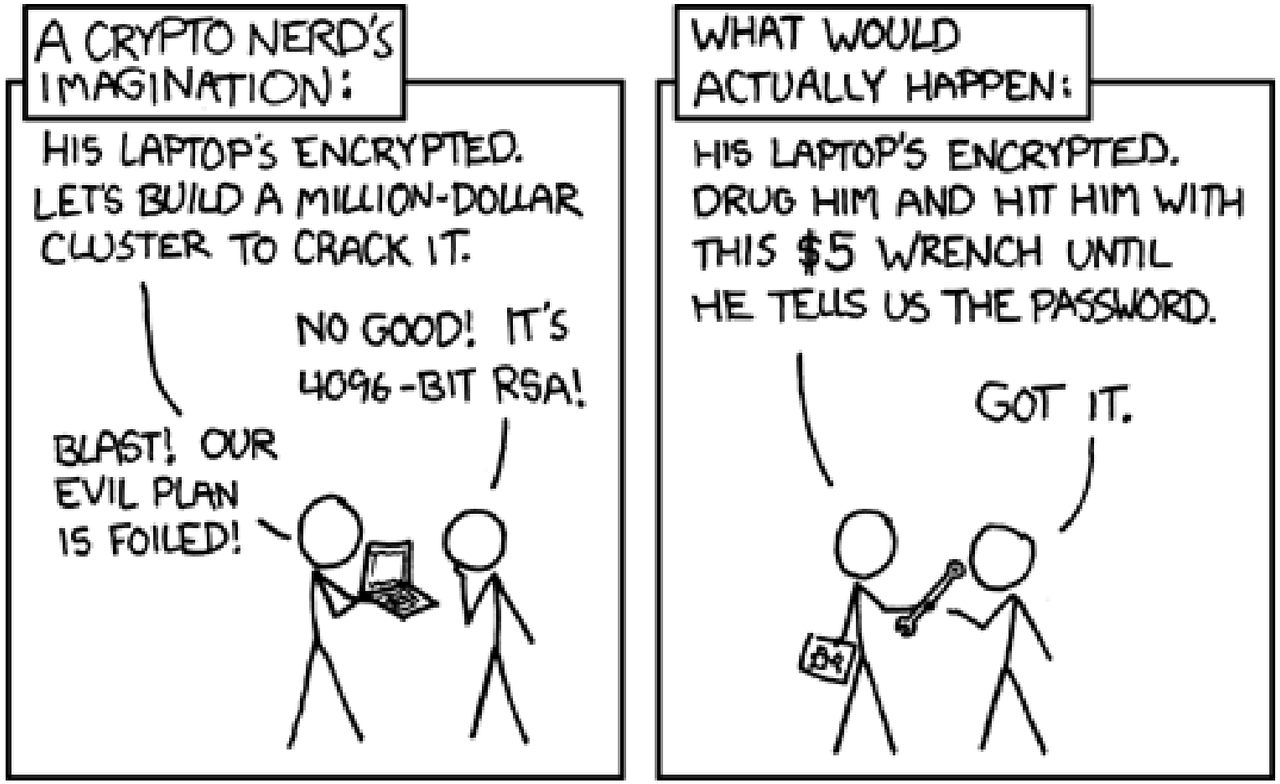
Strengths and Limitations

- Based on computational difficulty
- Efficient in classical environments
- Limited resilience against quantum attacks

Quantum Computing Vs Cryptography

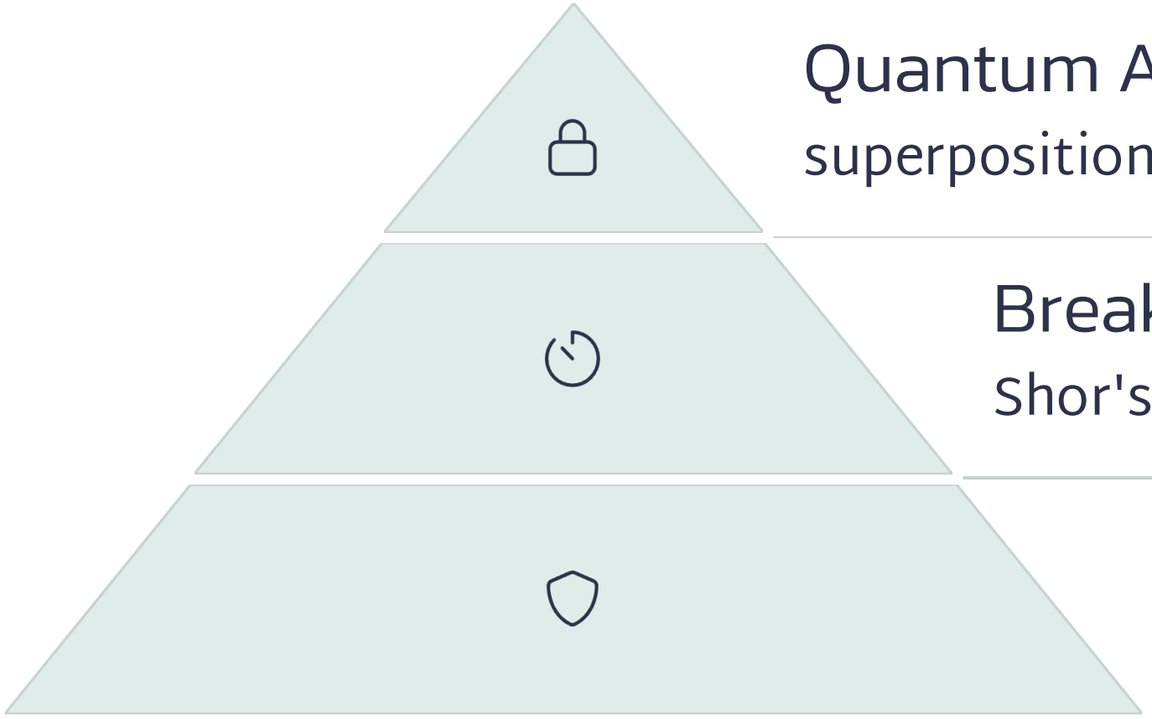
How Quantum Computing Can Break Encryption?

NOT Like THIS



https://xkcd.com/538/

How Quantum Computing Can Break Encryption?



Quantum Advantage

superposition and entanglement

Breaking Encryption

Shor's algorithm breaks RSA and ECC in hours

Critical Vulnerabilities

Communications and infrastructure at risk

Quantum Algorithms (Examples of Potential)

Demonstrating quantum superiority:

- **Shor's Algorithm (1994):**
  - **Purpose:** Efficiently factorizes large numbers.
  - **Impact:** Threatens current RSA, DSA, ECC, DH, and El Gamal; requires quantum-safe cryptography.
  - Breaks TLS encryption, digital signatures, SSH, VPNs, and even cryptocurrencies.

Problem	Classical Time	Quantum (Shor's) Time
Factor 2048-bit RSA	>10^20 years	Hours or minutes
ECC Discrete Logarithm	Infeasible	Feasible

- **Grover's Algorithm (1996):**
  - **Purpose:** Speeds up unstructured database search.
  - **Speedup:** Quadratic speedup (N vs. N).
  - **Impact:** Optimizing search and data analysis. Can break Symmetric key encryption, including AES, ARIA, and DES3. Hash outputs as well

Attack Scenarios

Attack Scenario 1 - HTTPS/TLS Interception

- Harvest now, decrypt later
- Long-term confidentiality risk

Attack Scenario 2 - Mobile Authentication

- Forging digital signatures
- Compromising app logins and messages

Attack Scenario 3 - Blockchain & Crypto

- Breaking wallet security
- Stealing crypto-assets

Breaking Modern AppSec

Shor's Algorithm

Can break RSA and ECC encryption exponentially faster than classical methods

Authentication Risk

Digital signatures and certificates become vulnerable

TLS Vulnerable

Secure communications channels could be compromised

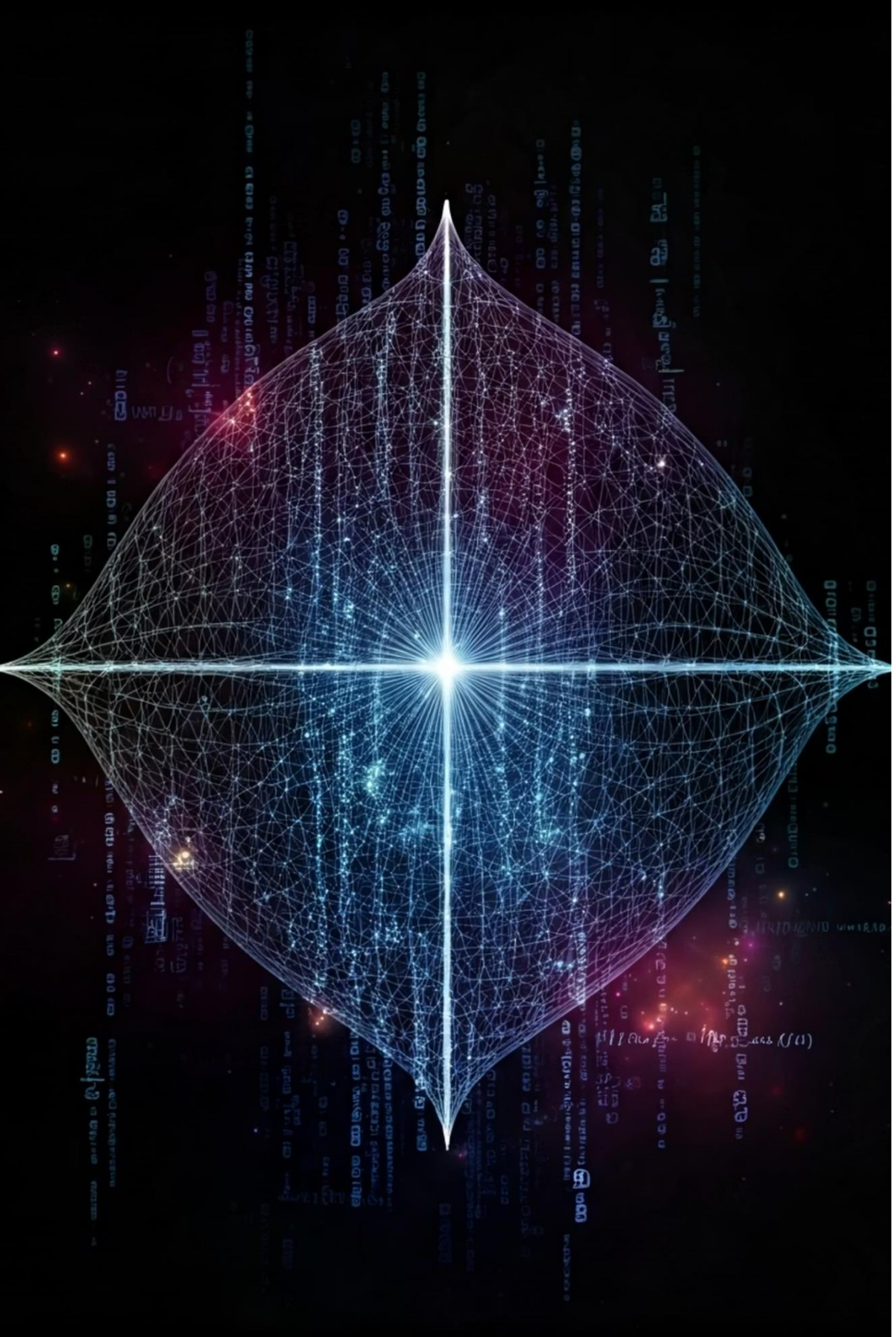
Data Exposure

Encrypted data stores may be decryptable retroactively

Post-Quantum Cryptography: The Next Frontier

Quantum computers threaten today's cryptography standards. Post-quantum cryptography (PQC) will protect sensitive data from future quantum attacks.

A global cryptographic transition is now urgent. Organizations must prepare for this security paradigm shift.



What Is Post-Quantum Cryptography (PQC)?

Quantum-Resistant Security

Secure against both quantum and classical attack vectors

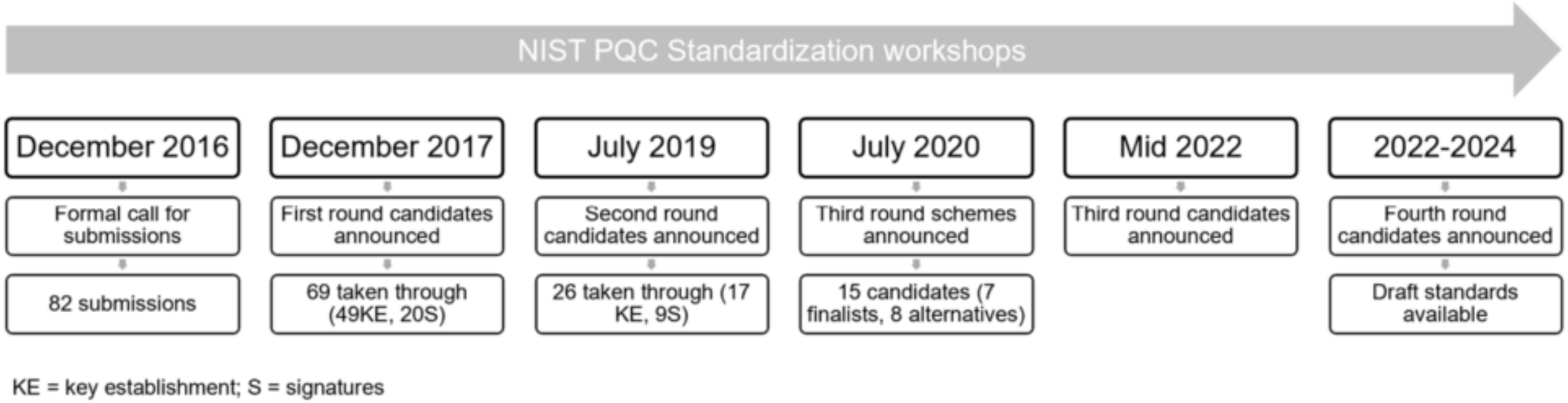
Complex Mathematics

Uses problems quantum computers can't easily solve

Practical Implementation

Designed for seamless integration with existing IT systems

NIST PQC Progress

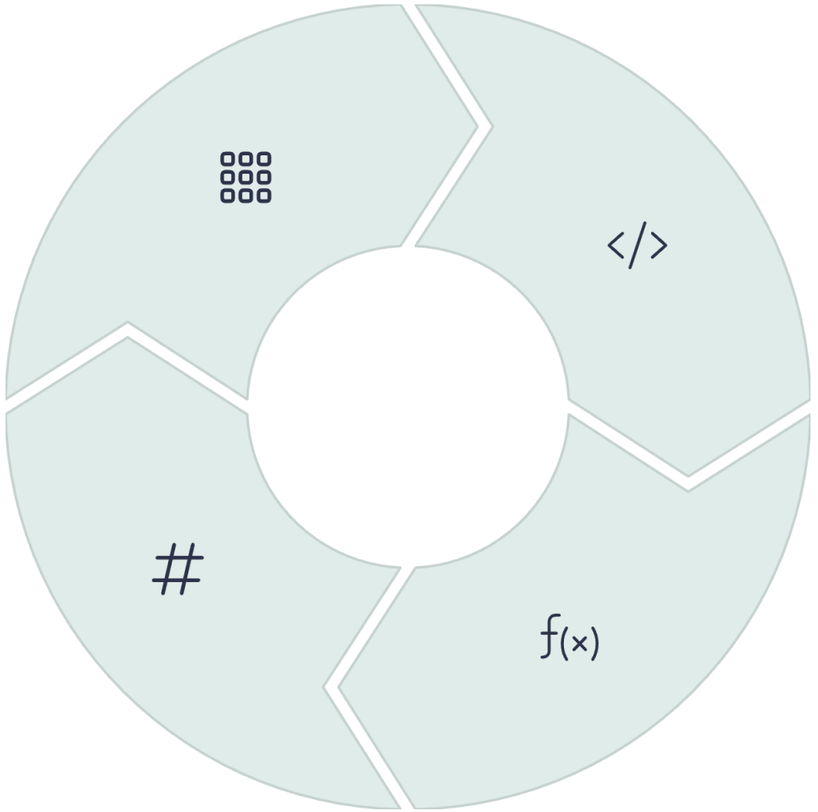


https://csrc.nist.gov/projects/post-quantum-cryptography
https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

Main Categories of PQC Algorithms

Lattice-based

CRYSTALS-Kyber,
CRYSTALS-Dilithium



Code-based

Classic McEliece

Hash-based

SPHINCS+

Multivariate

Rainbow

NIST PQC Standardization: Leading Algorithms

CRYSTALS-Kyber

Selected for encryption and key exchange. Offers excellent balance of security and performance.

- Lattice-based security
- Compact keys
- Efficient processing

CRYSTALS-Dilithium

Selected for digital signatures. Provides strong verification with reasonable size requirements.

- Fast verification
- Strong security proofs
- Implementation flexibility

Real-World Applications and Migration Challenges

Federal Mandates
U.S. agencies preparing for quantum-safe systems

Global Banking
Financial networks upgrading encryption standards

Cloud Infrastructure
Providers implementing quantum-resistant protocols

IoT Devices
Resource constraints require optimized algorithms

The Future: Safeguarding Data in a Quantum World

Awareness

Organizations must recognize quantum threats now. Security planning should include PQC roadmaps.

Collaboration

Government, industry, and academia must work together. Standards development requires diverse expertise.

Implementation

Proactive adoption is crucial. Organizations that start early gain security advantages.

Post-Quantum Cryptography

Lattice-Based

Uses high-dimensional mathematical lattices. NIST's top candidate for standardization.

Hash-Based

Builds signatures using hash functions. Simple but larger signature sizes.

Code-Based

Relies on error-correcting codes. Well-studied but requires larger keys.

Multivariate

Based on difficulty of solving multivariate polynomial equations. Compact signatures.

NIST is finalizing PQC standards. Several algorithms show promise for different use cases.

Quantum-Safe Migration Strategy

Cryptographic Inventory

Identify all crypto-dependent assets and algorithms

Risk Assessment

Evaluate data lifespan and quantum threat exposure

Crypto Agility

Implement systems that can rapidly switch encryption methods

Hybrid Approach

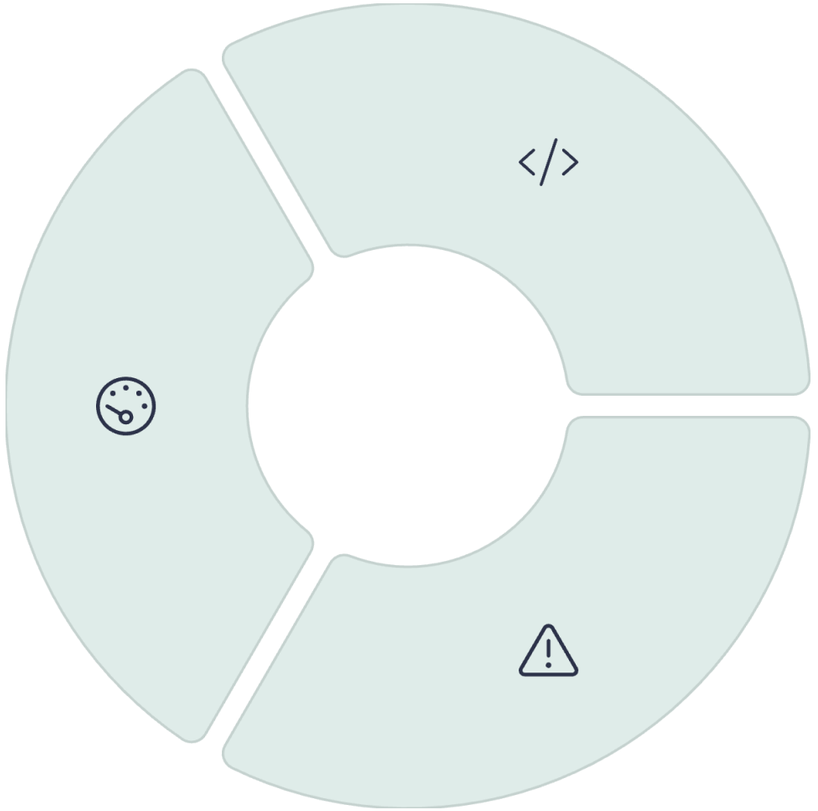
Deploy classical + post-quantum algorithms together

Implementation Challenges

Performance Impact

PQC algorithms require more computational resources

- Larger keys and signatures
- Increased processing time



Integration Complexity

Legacy systems present migration challenges

- Hardware dependencies
- Third-party components

Immature Standards

PQC standards still evolving

- Implementation uncertainty
- Potential algorithm vulnerabilities

Action Plan for AppSec Teams

Educate Your Organization

Build quantum computing awareness. Train security and development teams on PQC basics.

Update Security Requirements

Add quantum-resistance to security policies. Include PQC in vendor evaluations.

Start Proof-of-Concept Projects

Experiment with PQC libraries. Test performance and integration in non-production environments.

Engage with Standards Bodies

Follow NIST and other standardization efforts. Participate in industry working groups.

Post-Quantum Readiness Checklist

1. **Awareness & Education:**
   - Understand Shor's and Grover's threats to current crypto.
   - Identify systems using RSA, ECC, DH, DSA, or ElGamal.
   - Share learnings with teams.
2. **Cryptographic Inventory:**
   - List all encrypted/signature-based systems.
   - Document algorithms, key sizes, and certificate types.
   - Mark systems with long-term confidentiality needs.
3. **Risk Assessment:**
   - Evaluate the lifespan of sensitive data.
   - Identify 'harvest now, decrypt later' risks.
4. **Migration Preparation:**
   - Enable crypto agility in systems.
   - Test PQC algorithms (Kyber, Dilithium, SPHINCS+).
   - Consider hybrid approaches (classical + PQC).
5. **Industry Engagement:**
   - Follow NIST PQC updates.
   - Join security working groups.
   - Track vendor PQC adoption.
6. **Operational Readiness:**
   - Pilot PQC in test environments.
   - Measure performance and storage impacts
   - Update policies for PQC readiness in new procurements.

Thank You – Any Questions?

References

- https://www.nist.gov/cybersecurity/what-post-quantum-cryptography
- https://csrc.nist.gov/projects/post-quantum-cryptography
- https://quantumai.google/quantumcomputer
- https://research.ibm.com/blog/ibm-quantum-characterization-lab-tour
- https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/
- https://www.aboutamazon.com/news/aws/quantum-computing-aws-ocelot-chip
- https://blogs.iu.edu/sciu/tag/superposition/
- https://ncase.me/qc-outline/
- https://www.youtube.com/watch?v=e3fz3dqhN44
- https://www.youtube.com/watch?v=ni1x44mCgWE
- https://www.youtube.com/watch?v=RQWpF2Gb-gU
- https://www.youtube.com/watch?v=-UrdExQW0cs
- https://blogs.cisco.com/developer/how-post-quantum-cryptography-affects-security-and-encryption-algorithms