CSS/ENG
ASSOCIATION

01

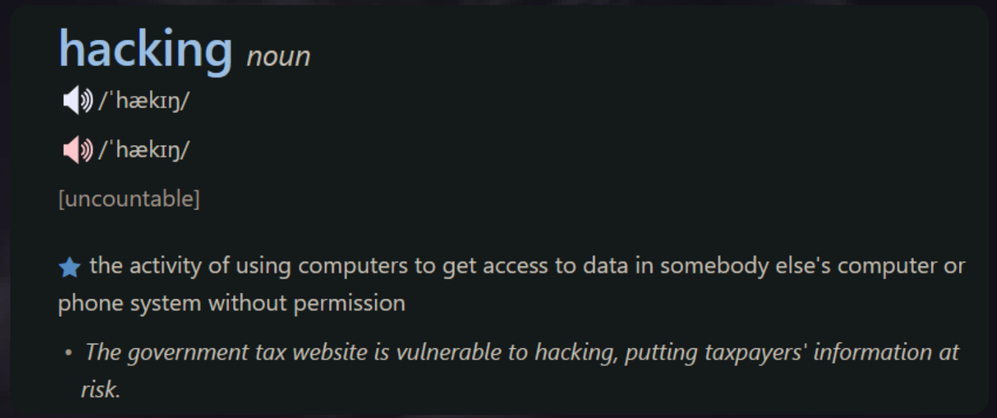


cybersecurity evolution

COMPUTER SCIENCE SOCIETY //WEEK 6

presented by aren, michal, sergi

Modern threat landscape



- The Evolution of Cyber Warfare: The era of “lone-wolf” hackers is largely over. Modern cyber threats are driven by Advanced Persistent Threats (APTs), state-sponsored intelligence agencies, and highly organized cybercriminal syndicates.

- Enterprise Risk: Breaches no longer just result in defaced websites. They lead to paralyzed critical infrastructure, intellectual property theft, and massive regulatory fines under frameworks like GDPR.

- Asymmetric Warfare: Cybersecurity is fundamentally asymmetric. A Security Operations Center (SOC) must defend millions of vulnerabilities and be successful 100% of the time. An attacker only needs to find one exploit, misconfiguration, or compromised credential to breach the perimeter.

Enterprise Defense Architecture

- Security Information and Event Management (SIEM): Corporations rely on SIEM platforms to aggregate terabytes of log data from firewalls, endpoints, and servers in real-time to detect anomalous behaviour.

- Endpoint Detection and Response (EDR): Traditional antivirus software relies on known malware signatures. Modern EDR uses behavioural analytics and machine learning to isolate devices the moment malicious lateral movement is detected.

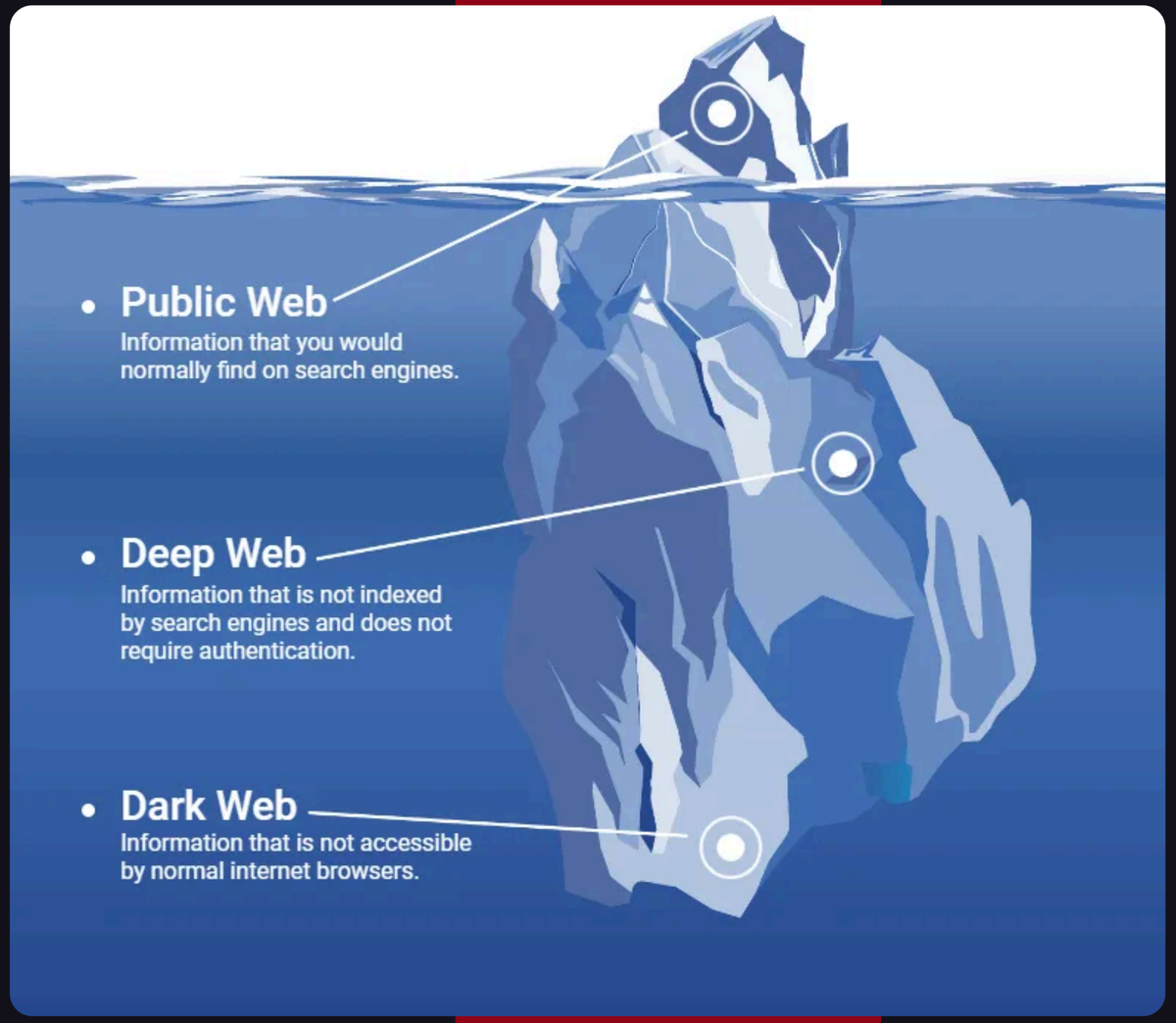
Zero Trust Architecture: The traditional "castle and moat" security model is obsolete. Zero Trust operates on the principle of "never trust, always verify," requiring strict identity verification for every person and device attempting to access resources, regardless of whether they are already inside the network perimeter.

The Anatomy of the Internet

- Public Web (approx. 4%): Content indexed by standard search engines (Google, Bing). This relies on web crawlers following hyperlinks and indexing HTML content.

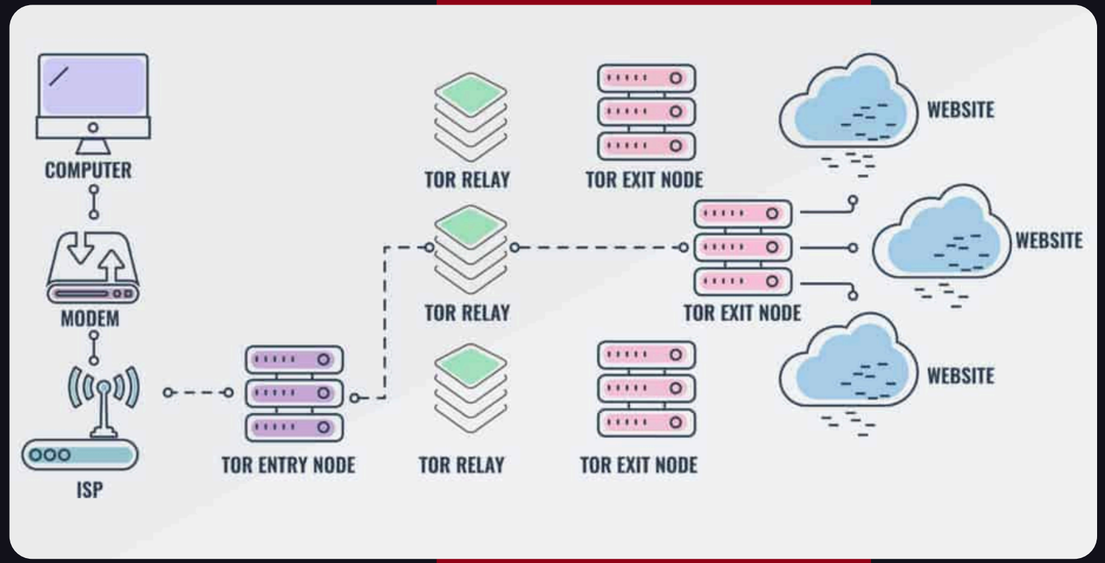
- Deep Web (approx. 90%+): Content dynamically generated or locked behind authentication protocols. This includes corporate databases, academic journals, secret internal government networks, and online banking infrastructures.

- Dark Web: Intentionally concealed overlay networks (darknets) that require specific, specialized software, configurations, or authorization to access. It utilizes non-standard routing protocols to ensure the anonymity of both the host and the user.



The Mechanics of Onion Routing (Tor)

- Standard TCP/IP Routing: In standard routing, packets contain the source and destination IP addresses in plaintext. Intermediary routers can see who is communicating with whom.
- The Tor Architecture: Traffic is routed through a decentralized network of volunteer-operated servers.
- The Node Sequence:



Guard Node: The entry point. Knows your IP address, but not your final destination.

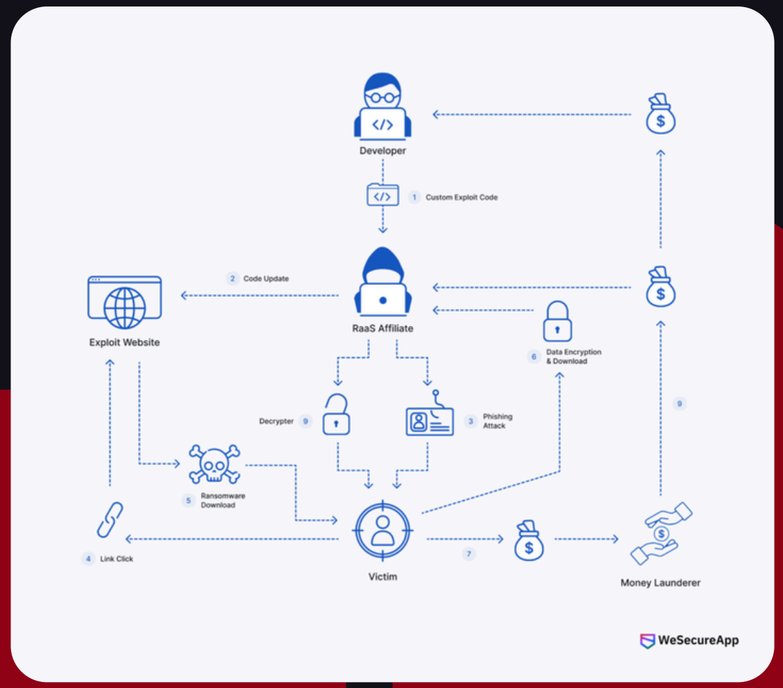
Middle Node: Knows the Guard Node and the Exit Node, but neither the source nor the destination.

Exit Node: Decrypts the final layer and sends traffic to the destination. Knows the destination, but not the original source.

Vulnerabilities: Exit nodes can be malicious. If traffic leaves the exit node unencrypted (HTTP), the node operator can intercept credentials and packet payloads.

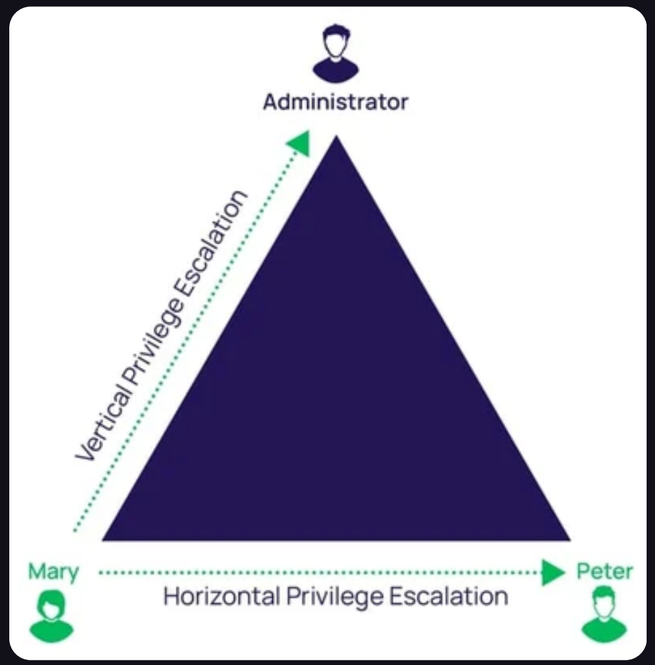
The Economics of Cybercrime (RaaS)

06

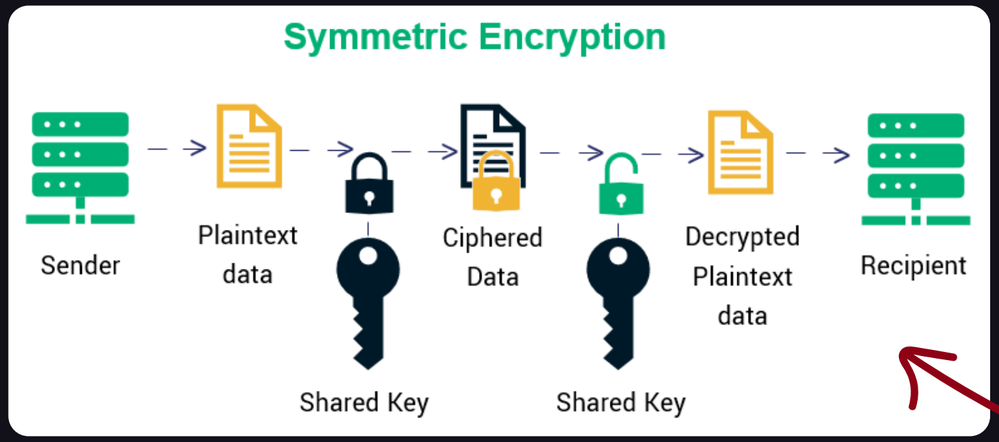


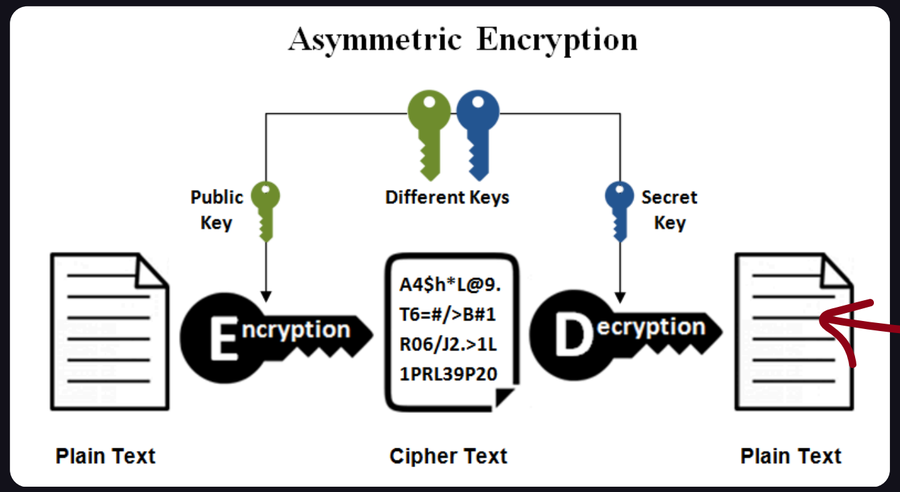
- Ransomware-as-a-Service (RaaS): Cybercrime has adopted a SaaS (Software-as-a-Service) business model. Malware developers write sophisticated encryption software and lease it to "Affiliates."
- Initial Access Brokers (IABs): Specialized hackers whose sole job is to breach networks, quietly escalate privileges, and then sell that persistent access on darknet forums to RaaS affiliates.
- The Extortion Economy: Modern ransomware utilizes "Double Extortion." The malware encrypts the organization's data (halting operations) and simultaneously exfiltrates it. If the ransom isn't paid for the decryption key, the data is leaked publicly, triggering massive regulatory fines and reputational destruction.

Attack Vectors & Privilege Escalation



- Social Engineering: The exploitation of human psychology to bypass technical security controls. Often highly targeted (Spear-Phishing) using Open Source Intelligence (OSINT) gathered from platforms like LinkedIn to impersonate executives.
- Lateral Movement: Once initial access is gained (often via a low-level employee's compromised machine), attackers do not strike immediately. They map the network, seeking servers and domain controllers.
- Privilege Escalation: Attackers exploit misconfigurations or kernel vulnerabilities to elevate their account permissions from a standard user to a Domain Administrator, granting them total control over the enterprise infrastructure.



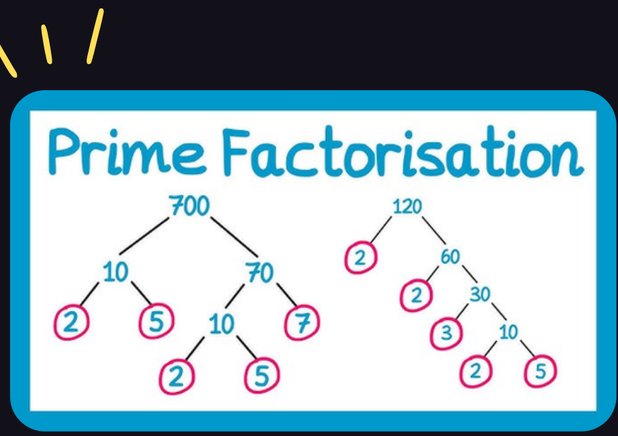


- Hashing: A one-way mathematical function that maps data of arbitrary size to a fixed-size bit array (e.g. SHA-256). Used for verifying data integrity and securely storing passwords. It cannot be mathematically reversed.
- Symmetric Encryption: Uses a single, shared key for both encryption and decryption (e.g. AES-256). It is computationally highly efficient and used for encrypting bulk data, but suffers from the "Key Distribution Problem."
- Asymmetric Encryption: Uses a mathematically linked key pair: a Public Key (for encryption) and a Private Key (for decryption). It solves the key distribution problem but is significantly slower and more computationally expensive than symmetric encryption.

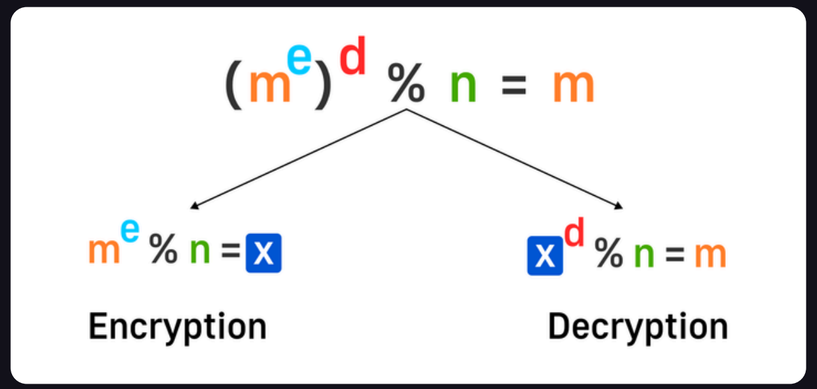
Cryptographic Primitives

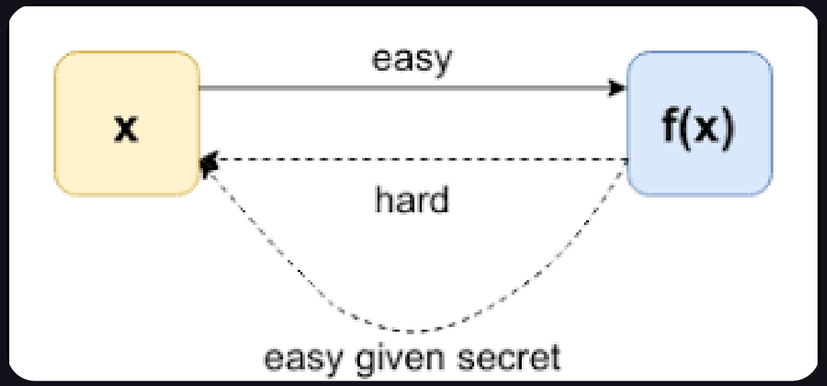


The Mathematics of RSA (Encryption & Decryption)



- Step 5: The Private Exponent: Compute d, the modular multiplicative inverse of e modulo phi(n).
  - This is expressed as: de equivalent to 1 pmod phi(n)
- The Keys: Your Public Key is the pair (n, e). Your Private Key is the pair (n, d).
- Encryption: To encrypt a message m (where m < n), the sender computes the ciphertext c.





- The Trapdoor: Anyone can encrypt using e and n. But without knowing phi(n) - which requires knowing the original primes p and q - it is computationally unfeasible to derive d and decrypt c.

The Mathematics of RSA (Key Generation)

RSA relies on the computational difficulty of integer factorisation - specifically, the product of two incredibly large prime numbers.

Choose two distinct, very large prime numbers, and q (typically 2048 bits long).

Modulus: Calculate n = p times q. This n will be used as the modulus for both the public and private keys. Its length determines the key length.

Euler’s Totient Function: Calculate phi(n). Since p and q are prime, phi(n) = (p-1)(q-1).

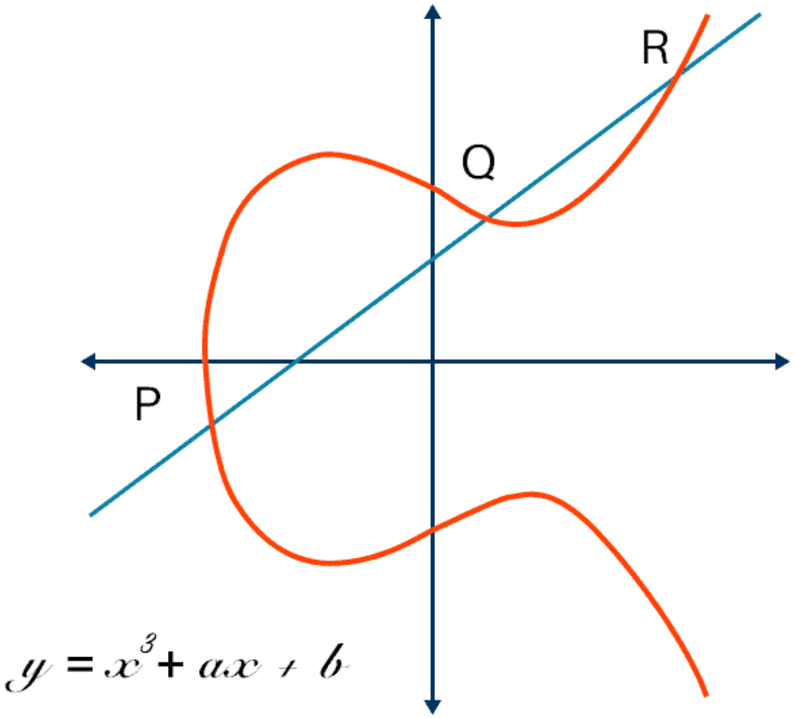
Public Exponent: Choose an integer e such that 1 < e < phi(n), and e is coprime to phi(n).

Euler's Product Formula

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Elliptic-Curve Cryptography 11

The Alternative to RSA: While RSA relies on prime factorisation, ECC relies on the algebraic structure of elliptic curves over finite fields.



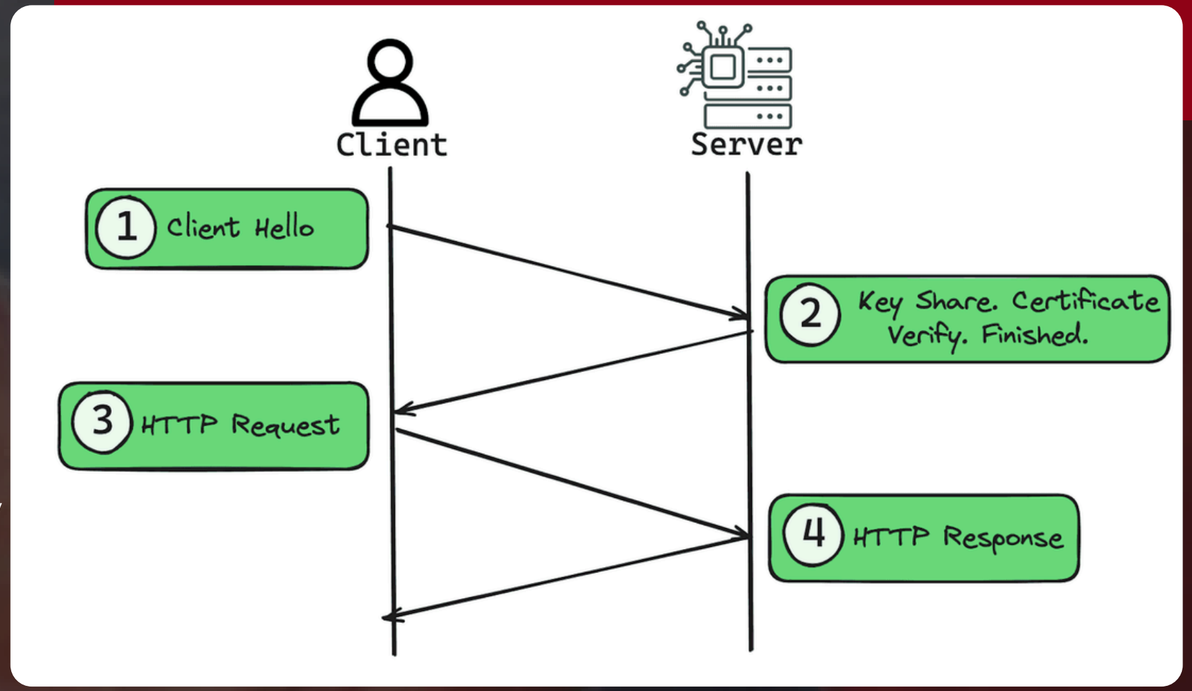
- The Advantage: ECC provides the same level of cryptographic security as RSA but with vastly smaller key sizes. A 256-bit ECC key offers comparable security to a 3072-bit RSA key.
- Real-World Application: Because of its low computational overhead as well as low memory requirements, ECC is the standard for mobile device security and cryptocurrencies like Bitcoin.

The TLS/SSL Handshake in Action

How browsers establish a secure, encrypted connection with a server over the public internet in milliseconds:

12

1. The browser and server exchange supported cipher suites and a string of random bytes.
2. (Authentication & Asymmetric Key Exchange): The server sends its SSL certificate (containing its RSA Public Key). The client verifies the certificate with a Certificate Authority.
3. The client encrypts a "Premaster Secret" using the server's Public Key. Only the server's Private Key can decrypt it. Both sides use this secret to mathematically generate identical Symmetric Session Keys.
4. Asymmetric encryption is abandoned. The rest of the session is encrypted using the blazing-fast Symmetric Session Keys.

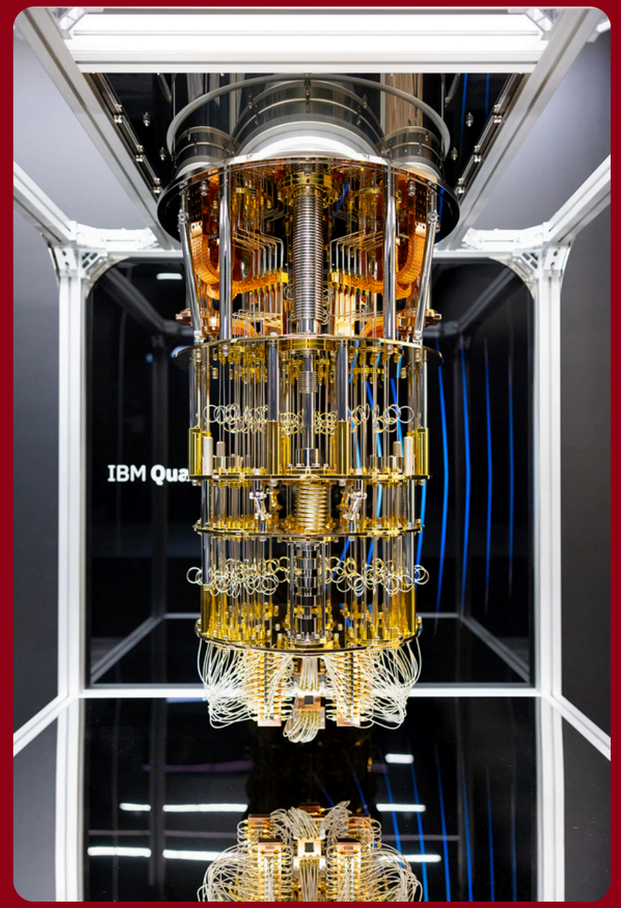


The Quantum Threat

- RSA and ECC are currently secure because classical computers cannot efficiently factorize large integers or solve discrete logarithms.

- Classical bits exist as 0 or 1. Quantum bits (Qubits) can exist in a state of superposition (representing both 0 and 1 simultaneously) and can be entangled, allowing for exponential parallel processing.

- Shor's Algorithm: A quantum algorithm formulated by Peter Shor in 1994. It proves that a quantum computer could solve prime factorization in polynomial time, effectively breaking RSA and ECC almost instantly.



- The Ticking Clock: Quantum computers capable of breaking RSA (Cryptographically Relevant Quantum Computers) do not yet exist. However, the threat is current.

- Data Harvesting: State-sponsored actors are currently intercepting and storing massive volumes of encrypted geopolitical, military, and corporate data.

- The Strategy: While they cannot read the data today, they are storing it in data centers with the intent to decrypt it years later when quantum technology matures.



INDUSTRY NEWS • DIGITAL PRIVACY • 2 min read •

Germany Halts EU's 'Chat Control' Push in Defense of Digital Privacy

Vlad CONSTANTINESCU
October 09, 2025

Berlin's firm opposition deals a decisive blow to Brussels' plan for mass message scanning.

Germany's stand against intrusive monitoring

Germany has formally opposed the European Union's proposed "Chat Control" regulation, a controversial measure that would require messaging platforms to scan private communications for illegal content. The law, which would have applied to encrypted chats, has faced mounting criticism from privacy advocates, technologists and human rights organizations.

Jens Spahn of Germany's Christian Democratic Union confirmed that Berlin would not support a policy that effectively mandates mass surveillance. He compared it to "opening all letters as a precautionary measure," saying the measure crosses a fundamental privacy line. With Germany representing roughly 19 percent of the EU's population, its stance almost guarantees the proposal's failure under EU voting rules.

"Harvest Now, Decrypt Later"

Post-Quantum Cryptography (PQC)

The Future of Encryption

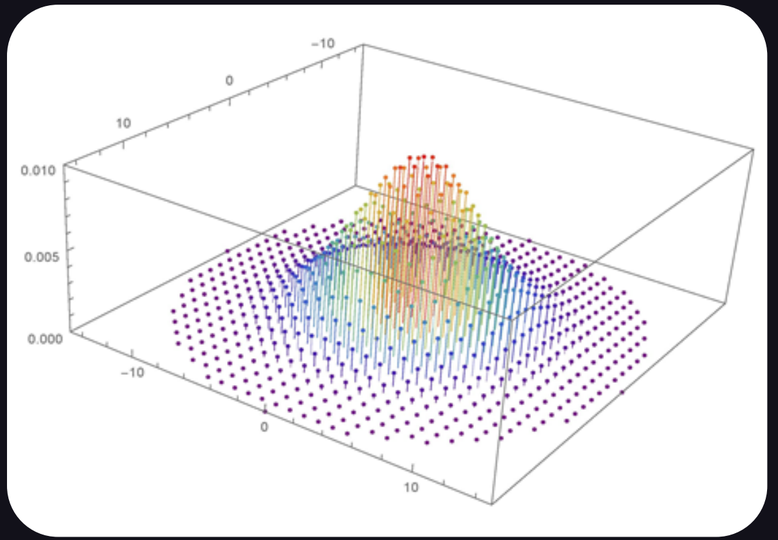
Mathematicians and computer scientists are actively developing new cryptographic algorithms that are secure against both classical and quantum computers.

Lattice Cryptography

The leading candidate for PQC. Instead of factoring primes, it involves finding the shortest vector in a highly complex, multidimensional mathematical lattice - a problem that even quantum computers struggle to solve efficiently.

NIST Standards

The National Institute of Standards and Technology (NIST) has already begun standardizing these post-quantum algorithms to prepare global infrastructure for the quantum transition.



CSS/ENG
ASSOCIATION



thank you for listening

The world is a dangerous place to live, not because of the people who are evil, but because of the people who don't do anything about it.”

— **Albert Einstein**

presented by aren, michal, sergi