CRYPTO 101: BUILDING BLOCKS

cryptography101.ca

Course outline

- V1: Introduction to cryptography
- V2: Symmetric-key encryption
- V3: Hash functions
- V4: Message authentication codes
- V5: Authenticated encryption
- V6: Public-key cryptography
- V7: RSA
- V8: Elliptic curve cryptography

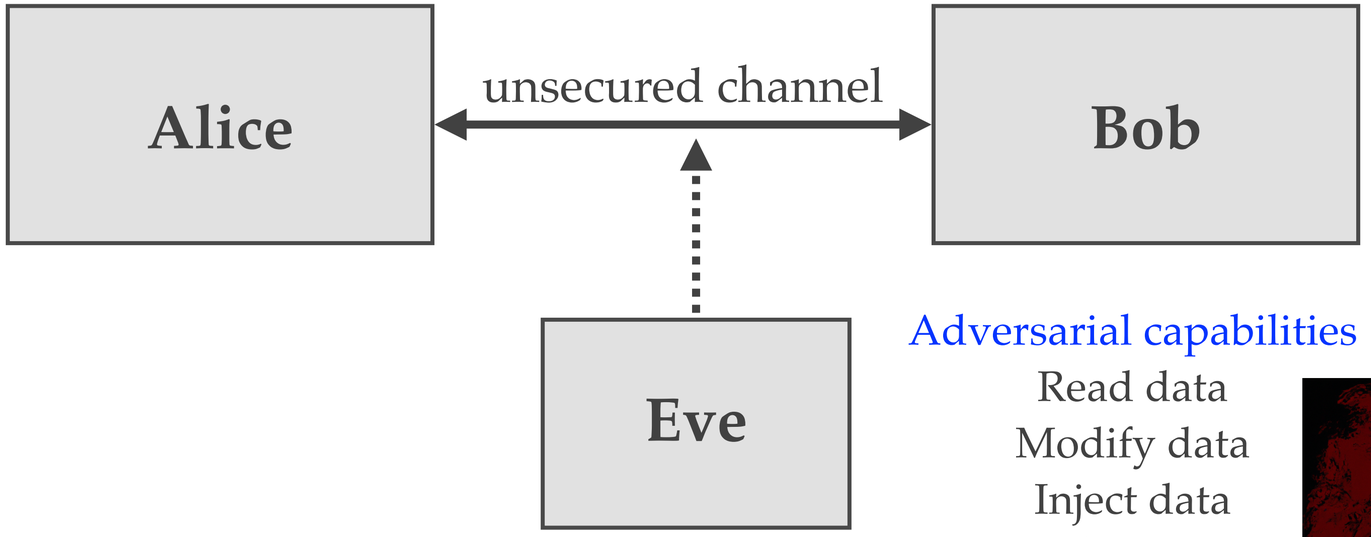
1 INTRODUCTION TO CRYPTOGRAPHY

CRYPTO 101: Building Blocks

cryptography101.ca

What is cryptography?

Cryptography is about securing communications in the presence of malicious adversaries.

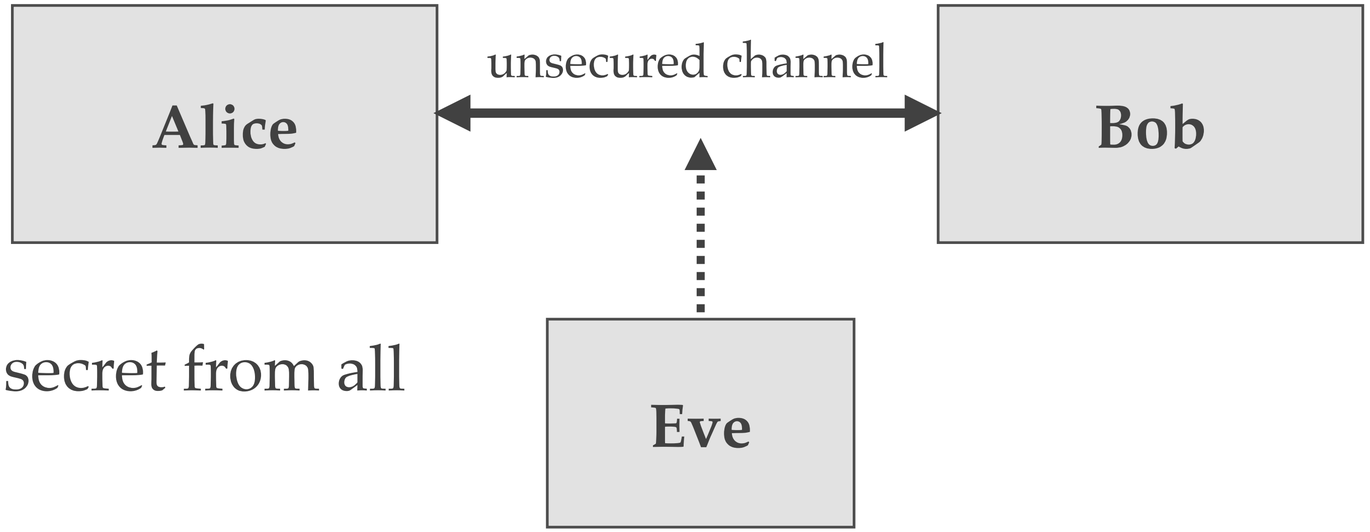


Adversarial capabilities (more than eavesdropping)

Read data
Modify data
Inject data
Delete data
……

The adversary is malicious, powerful, and unpredictable.

Fundamental goals of cryptography

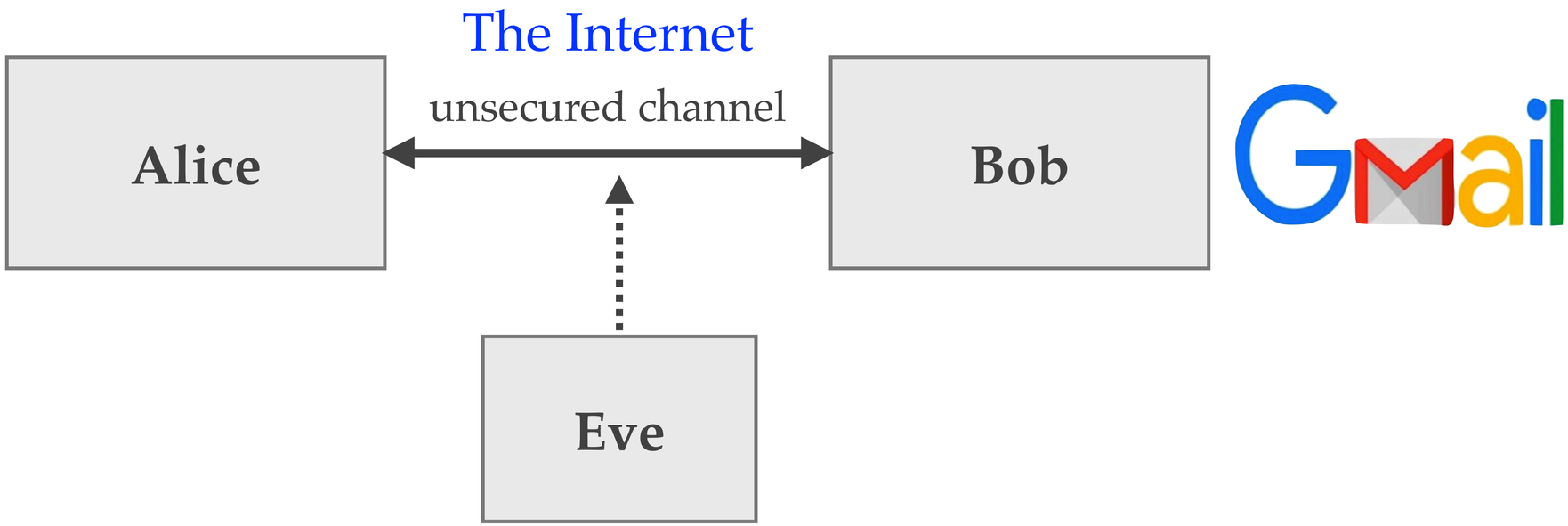


1. Confidentiality: Keeping data secret from all but those authorized to see it.
2. Data integrity: Ensuring data has not been altered by unauthorized means.
3. Data origin authentication: Corroborating the source of data.
4. Non-repudiation: Preventing an entity from denying previous commitments or actions.

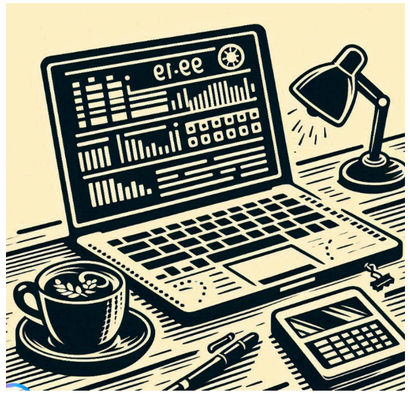
authentication

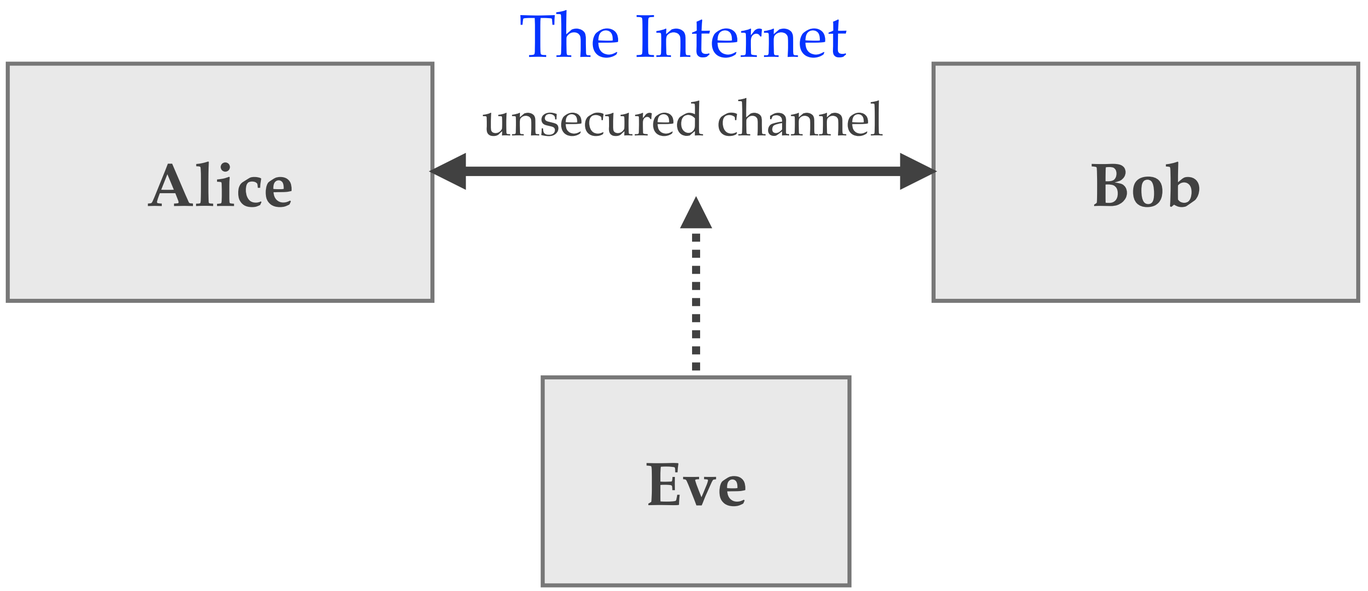
Secure browsing

TLS 1.3



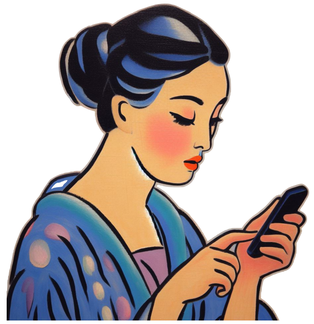
Automatic software upgrades

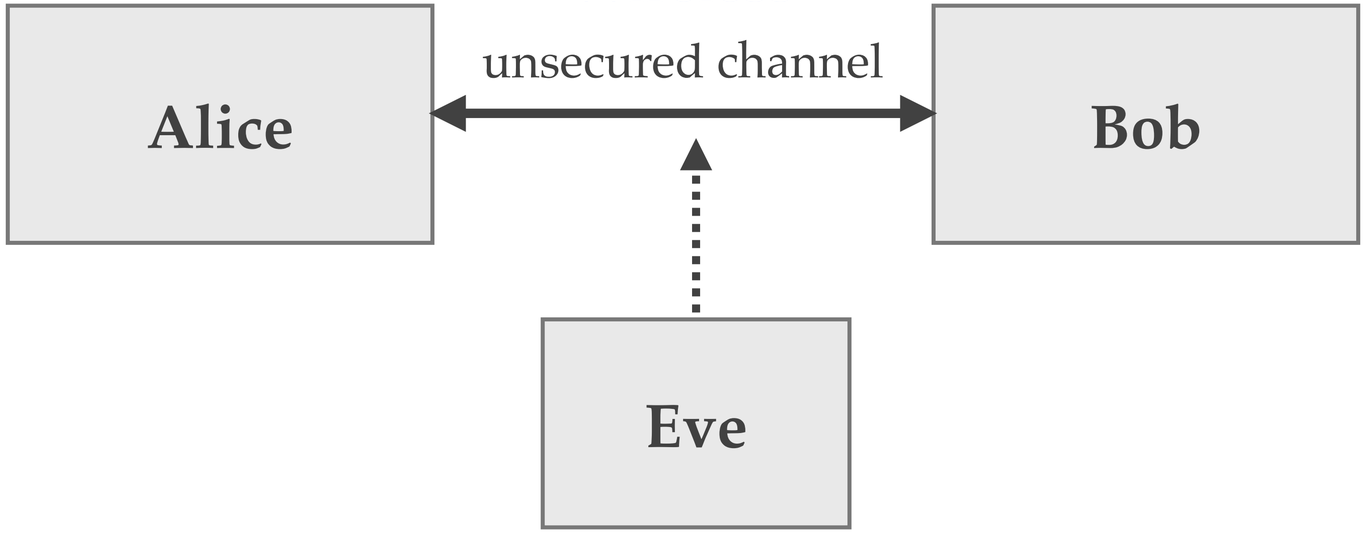


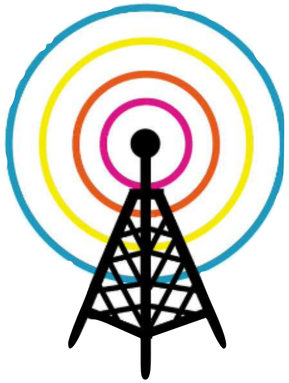


Microsoft

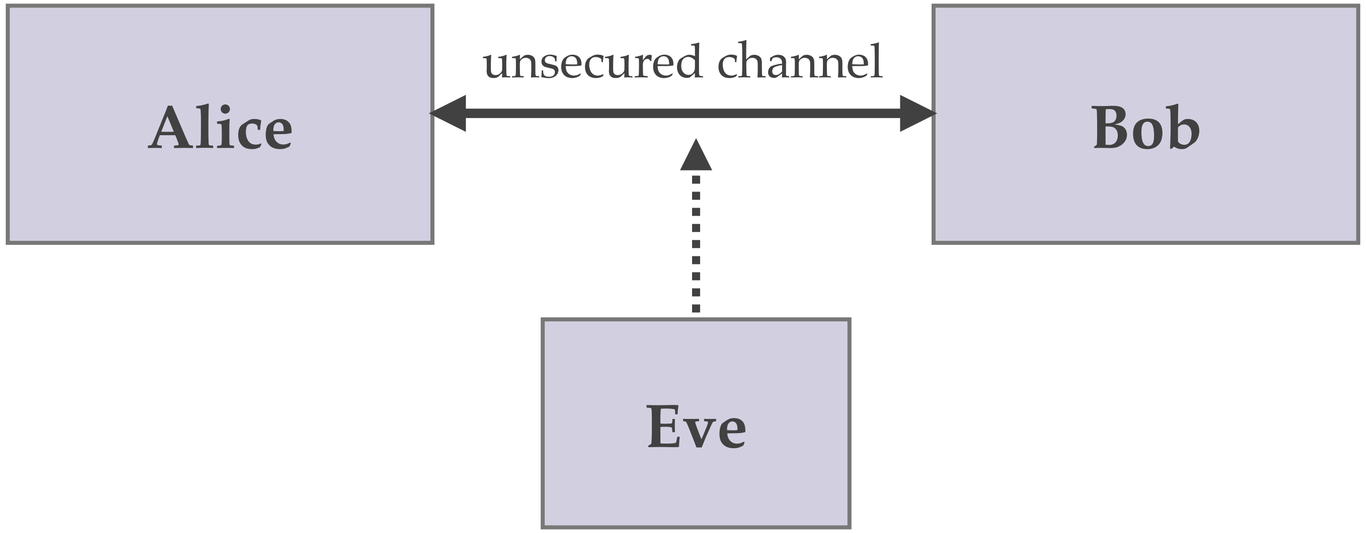
Cell phone service







Bluetooth



Secure messaging

Wired / Wireless

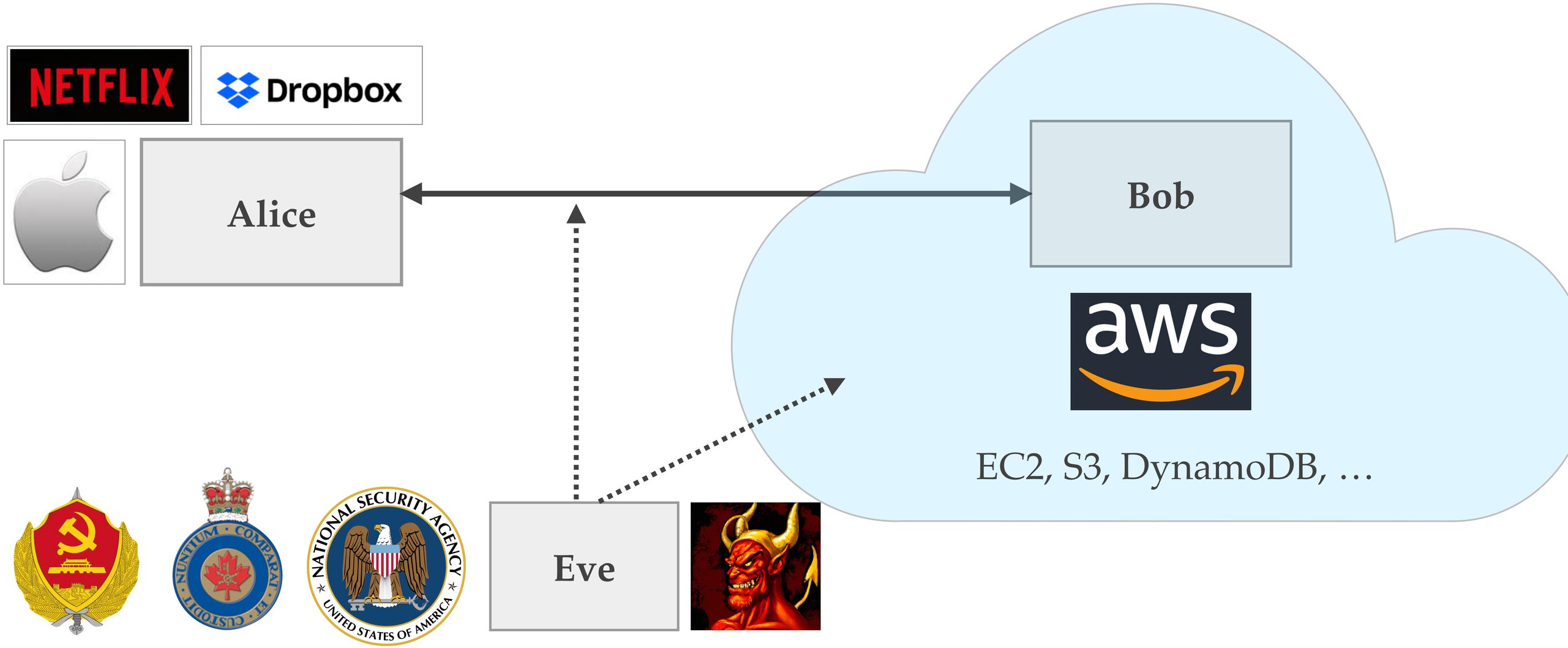
unsecured channel

Alice

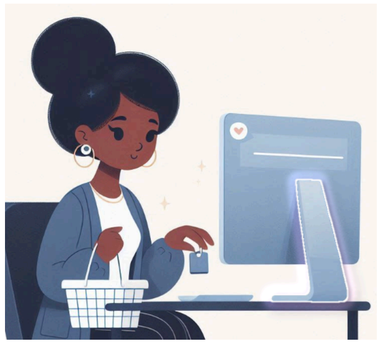
Bob

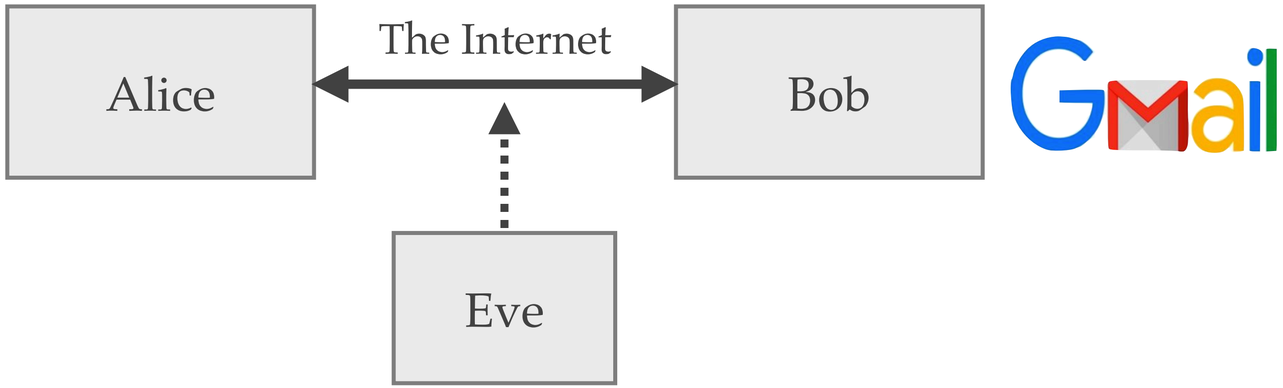
Eve

Cloud computing



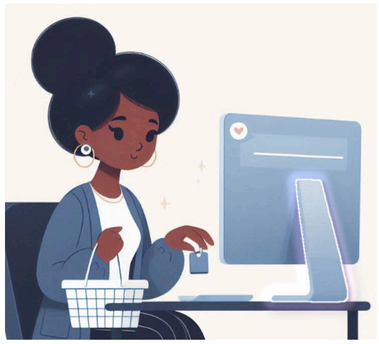
Secure web transactions

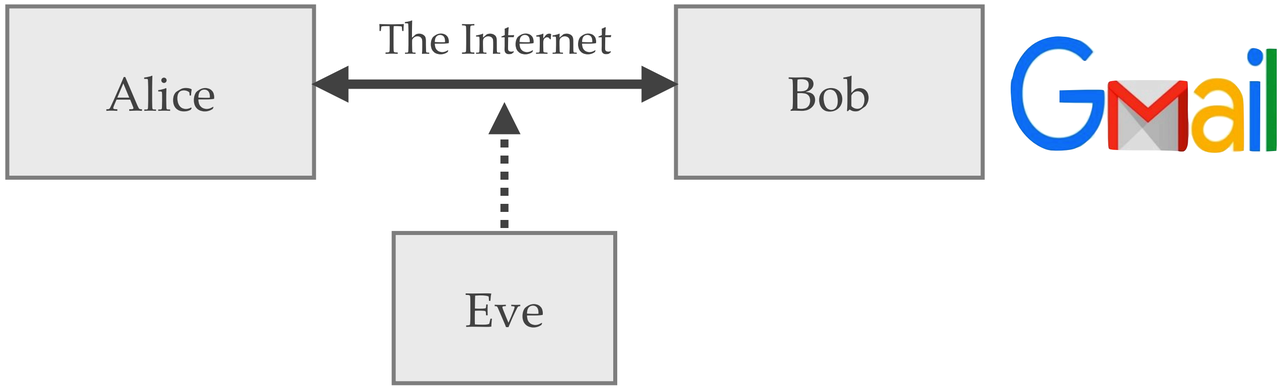




- Transport Layer Security (TLS): The cryptographic protocol used by web browsers to securely communicate with web sites such as gmail, facebook, amazon, etc.
- TLS is used to assure an individual user (client) of the authenticity of the web site (server) they are visiting, and to establish a secure communications channel for the remainder of the session.

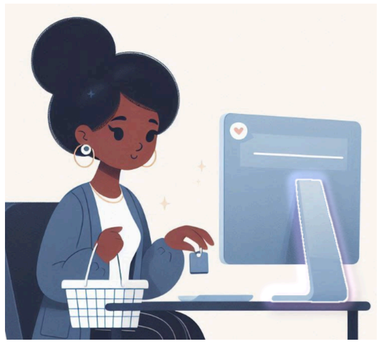
Secure web transactions (2)

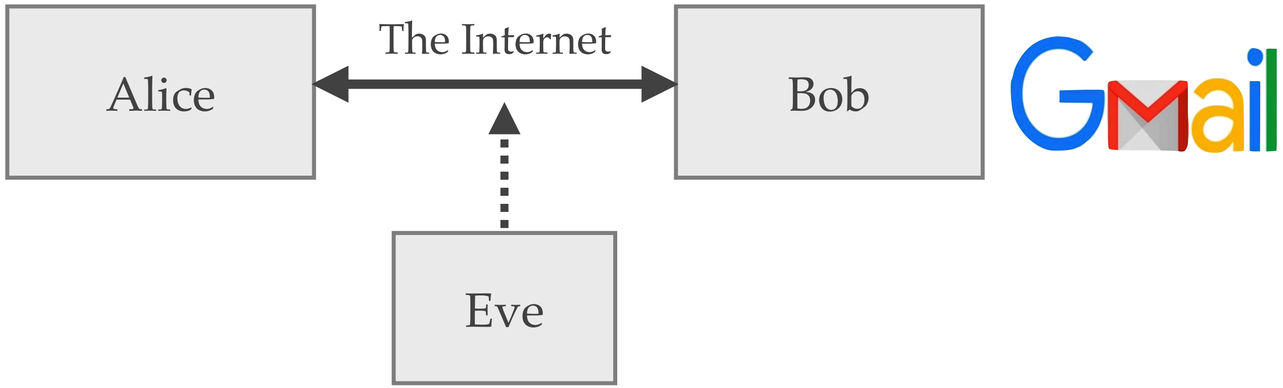




- Symmetric-key cryptography: The client and server a priori share some secret information k called a key.
- They can subsequently engage in secure communication by encrypting their messages with AES and authenticating the resulting ciphertexts with HMAC.
- **Question**: How do Alice and Bob establish the shared secret key k?

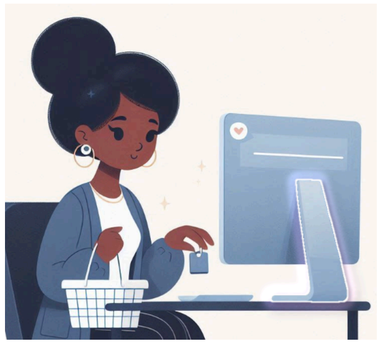
Secure web transactions (3)

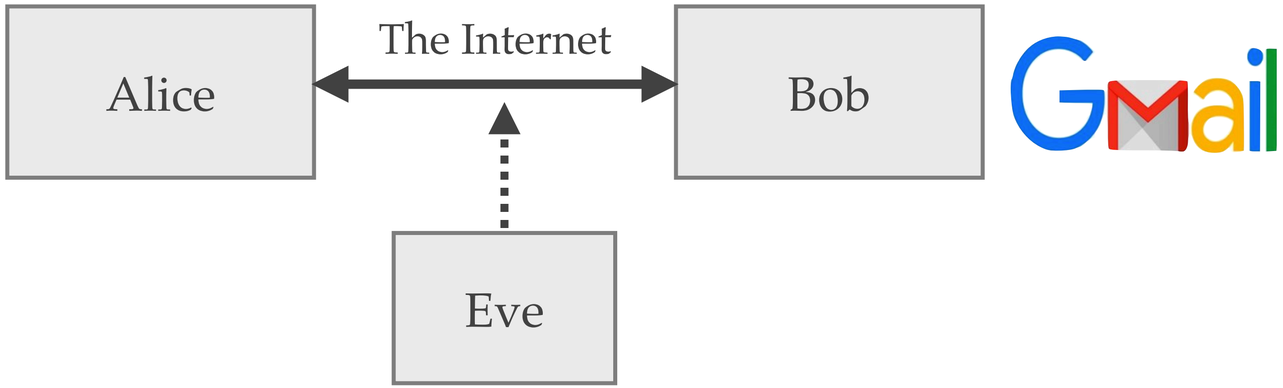




- Public-key cryptography: The client and server a priori share some authenticated (but non-secret) information.
- To establish a secret key, Alice selects the secret session key k, and encrypts it with Bob's RSA public key. Then only Bob can decrypt the resulting ciphertext with its RSA private key to recover k.
- **Question**: How does Alice obtain an authentic copy of Bob's RSA public key?

Secure web transactions (4)





- Signature scheme: Bob's RSA public key is signed by a Certification Authority (CA) using its secret signing key with the RSA signature scheme.
- Alice can verify the signature using the CA's RSA public verification key.
  In this way, Alice obtains an authentic copy of Bob's RSA public key.
- **Question**: How does Alice obtain an authentic copy of the CA's RSA public key?
- **Answer**: The CA's RSA public key is embedded in Alice's browser.

The TLS protocol

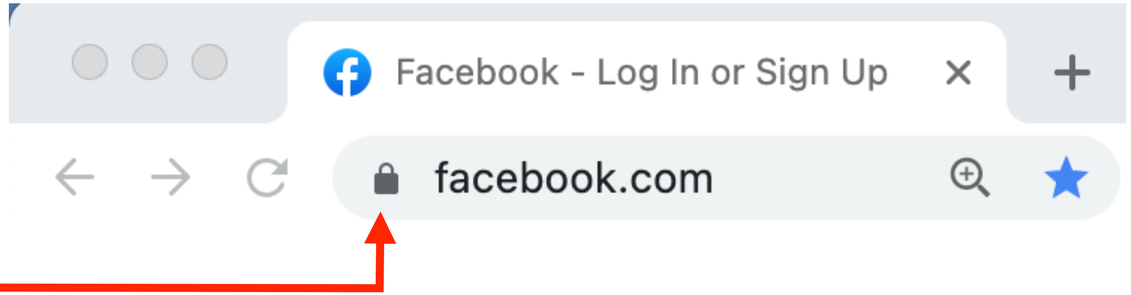
1. When a client first visits a secured web page, the server transmits its certificate to the client.
   - The certificate contains the server's identifying information (e.g. the web site name and URL) and RSA public key, and the RSA signature of a certification authority.
   - The certification authority (e.g. DigiCert) is trusted to carefully verify the server's identity before issuing the certificate.
2. Upon receipt of the certificate, the client verifies the signature using the certification authority's public key, which is embedded in the browser. A successful verification confirms the authenticity of the server and of its RSA public key.

The TLS protocol (2)

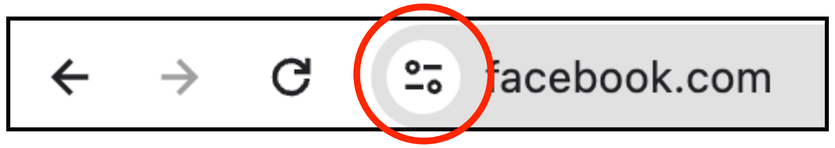
3. The client selects a random session key k, encrypts it with the server's RSA public key, and transmits the resulting ciphertext to the server.

4. The server decrypts the ciphertext to obtain the session key k, which is then used with symmetric-key encryption schemes to encrypt (e.g. with AES) and authenticate (e.g. with HMAC) all sensitive data exchanges for the remainder of the session.

5. The establishment of a secure link is indicated by a closed padlock in the browser.

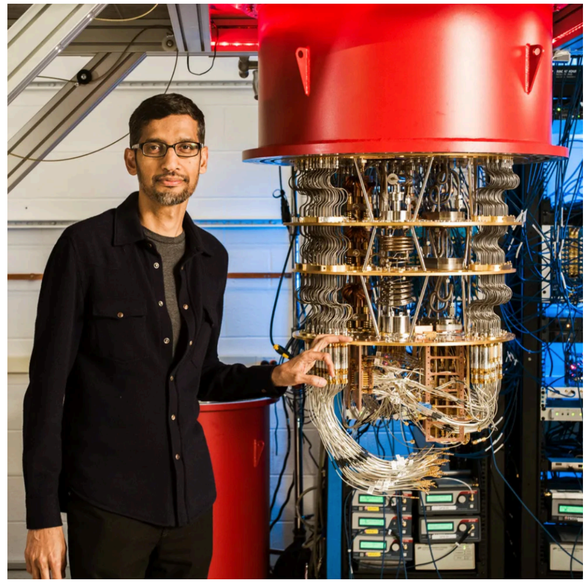


Chrome:



TLS potential vulnerabilities

There are many potential security vulnerabilities:

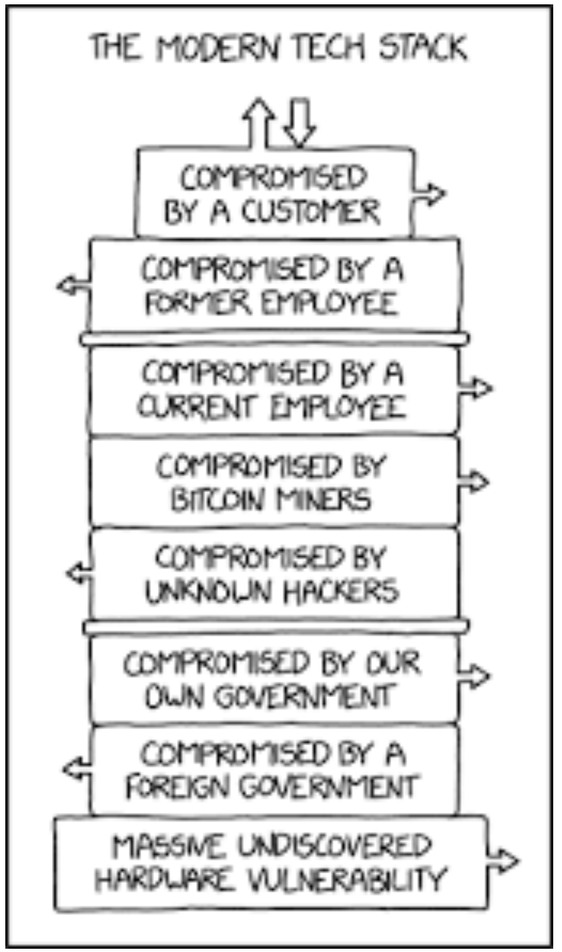


1. The crypto is weak (e.g. AES, HMAC, RSA).
2. The crypto can be broken using quantum computers.
3. Weak random number generation.
4. Issuance of fraudulent certificates.
   - In 2001, Verisign erroneously issued two Class 3 code-signing certificates to a person masquerading as a Microsoft representative.
5. Software bugs (both inadvertent and malicious).
6. Phishing attacks.
7. TLS only protects data during transit. It does not protect data stored at the server.

Cryptography in context

Cybersecurity is comprised of the concepts, technical measures, and administrative measures used to protect networks, computers, programs and data from deliberate or inadvertent unauthorized access, disclosure, manipulation, or use.

Also known as information security.



xkcd.com

Cybersecurity

COMPUTER SECURITY

- Security models and policies
- Secure operating systems
- Virus protection
- Auditing mechanisms
- Risk analysis
- Risk management

NETWORK SECURITY

- Internet protocols
- Viruses and worms
- Denial-of-service (DoS)
- Firewalls
- Intrusion detection
- Wireless communications

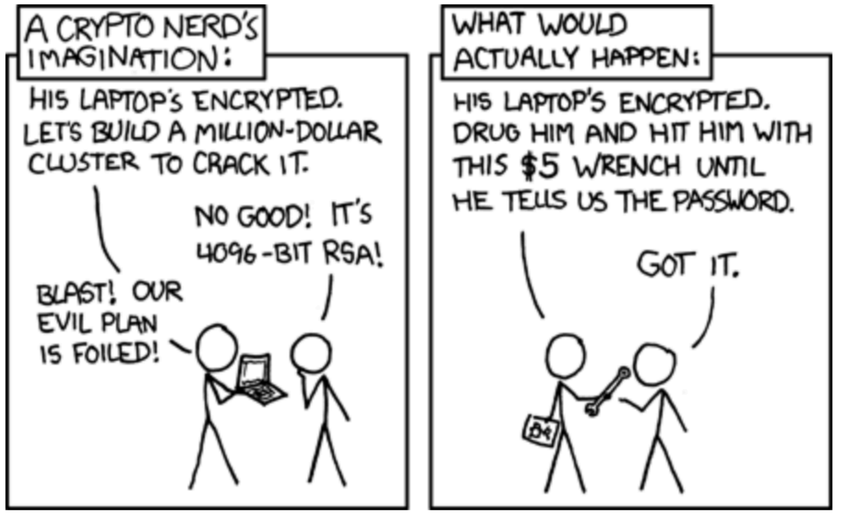
SOFTWARE SECURITY

- Buffer overflows
- Programming languages and compilers
- Digital rights management
- Code obfuscation
- Trusted computing

Cryptography ≠ Cybersecurity

- Cryptography provides some mathematical tools that can assist with the provision of cybersecurity services. It is a *small*, albeit *indispensable*, part of a complete security solution.
- Security is a chain 
  - Weak links become targets; one flaw is all it takes.
  - *Cryptography is usually not the weakest link.* However, when the cryptography fails, the damage can be catastrophic.
- *This course will focus on cryptography.*

xkcd.com

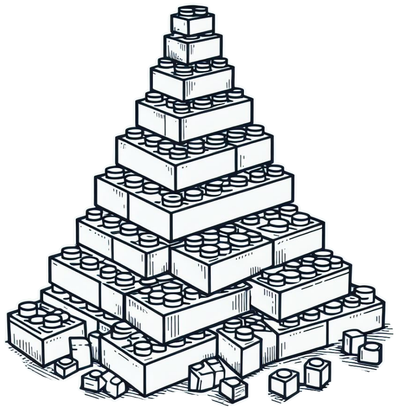


Syllabus (1)

Developer

Cryptographic Building Blocks

- Symmetric-key encryption
- Hash functions
- Message authentication
- Authenticated encryption
- Public-key encryption
- Digital signatures
- Key establishment
- RSA
- Elliptic curve cryptography



Apple's CryptoKit (September 2024)

- ChaCha20, AES
- SHA256, SHA384, SHA512
- HMAC
- AES-GCM, ChaCha20-Poly1305
- ECDSA,EdDSA
- P256, P384, P521, Curve25519
- ECDH
- HKDF

developer.apple.com/documentation/cryptokit/

Syllabus (2)

Crypto 101: Building Blocks

- Symmetric-key encryption
- Hash functions
- Message authentication
- Authenticated encryption
- Public-key encryption
- Digital signatures
- Key establishment
- RSA
- Elliptic curve cryptography

Crypto 101: Deployments

- GSM security
- AWS key management
- QQ browser security
- Bluetooth security
- Web security (TLS)
- Public-key infrastructure (PKI)
- Signal (WhatsApp)