Prof. Philip Koopman

Carnegie Mellon University

Electrical & Computer ENGINEERING

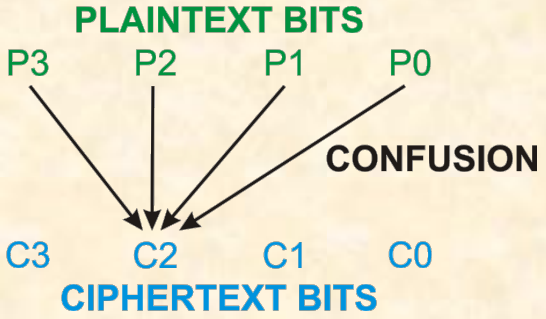
A Gentle Introduction to Cryptography

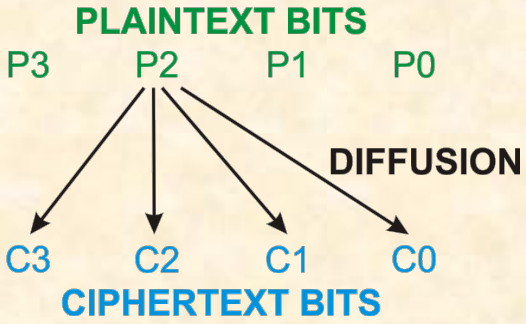
"Cryptography [without system integrity] is like investing in an armored car to carry money between a customer living in a cardboard box and a person doing business on a park bench."

– Gene Spafford

Cryptography Overview

- Anti-Patterns for Cryptography
  - Using a home-made cryptographic algorithm
  - Using private key when public key is required
  - Not considering key distribution in design
- Cryptography terms:
  - Plaintext: the original data
  - Ciphertext: data after a encryption
  - Encryption: converting plaintext to ciphertext
  - Avalanche effect:
    - Confusion: multiple bits in plaintext are combined to make a ciphertext bit
    - Diffusion: each bit of plaintext affects many bits of ciphertext
    - Ideally, ciphertext is random function of plaintext bits



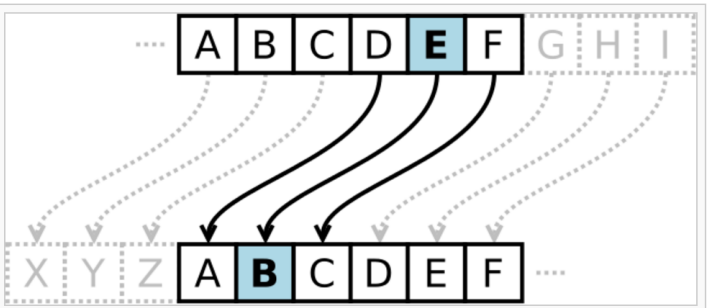


Classical Cryptography

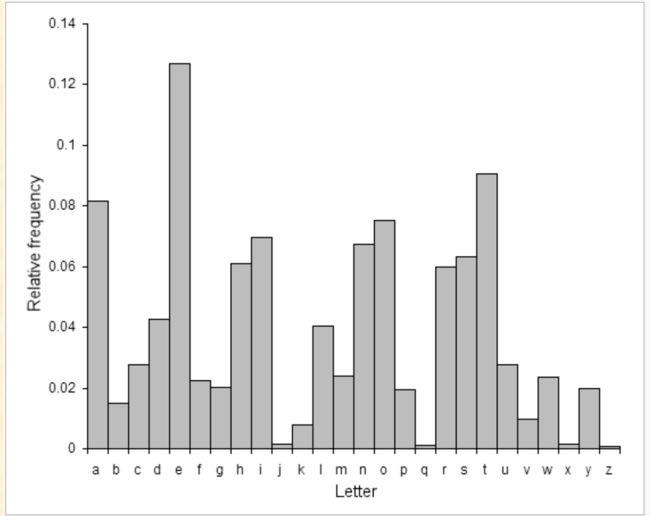
Carnegie Mellon University

- Simple substitution cipher (Caesar Cipher)
  - "IBM" left shifted 1 becomes "HAL" – 4 or 5 bit key (26 wheel positions)

https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung#/media/File:CipherDisk2000.jpg



The action of a Caesar cipher is to replace each plaintext letter with a different one a fixed number of places down the alphabet. The cipher illustrated here uses a left shift of three, so that (for example) each occurrence of E in the plaintext becomes B in the ciphertext. https://en.wikipedia.org/wiki/Caesar_cipher



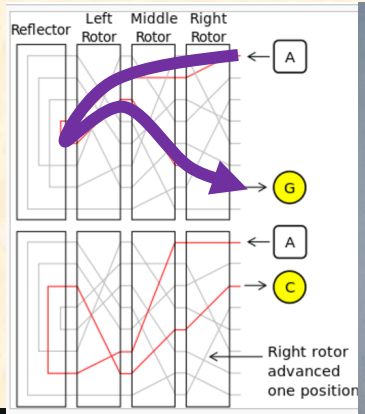
The distribution of letters in a typical sample of English language text has a distinctive and predictable shape. A Caesar shift "rotates" this distribution, and it is possible to determine the shift by examining the resultant frequency graph. https://en.wikipedia.org/wiki/Caesar_cipher

- Readily broken via frequency analysis
  - Most common letters correspond to E, T, A, O, …
  - Gives secrecy but not explicit integrity

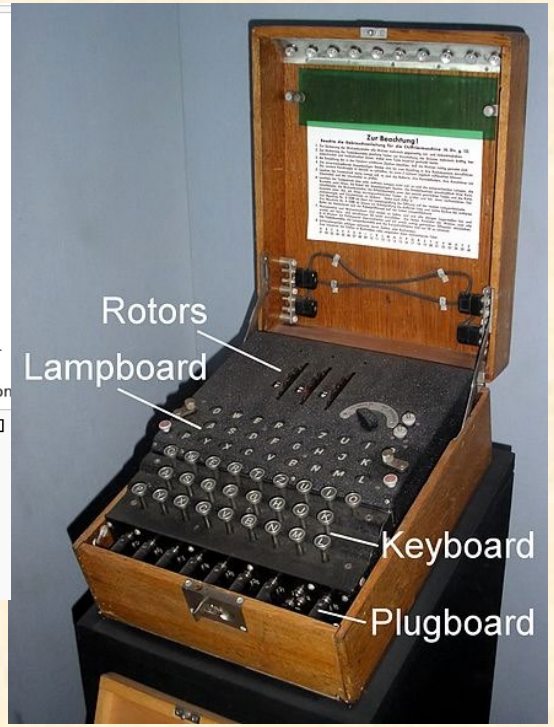
WWII Cryptography

Carnegie Mellon University

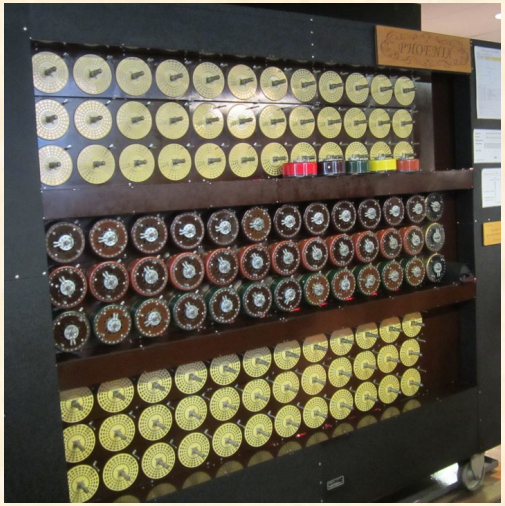
- Complex Subsitution Cipher
  - German “Enigma” machine
- The “Bombe” broke Enigma
  - Electromechanical sequencing to search for correlations using guessed plaintext
    - See the movie: “The Imitation Game”

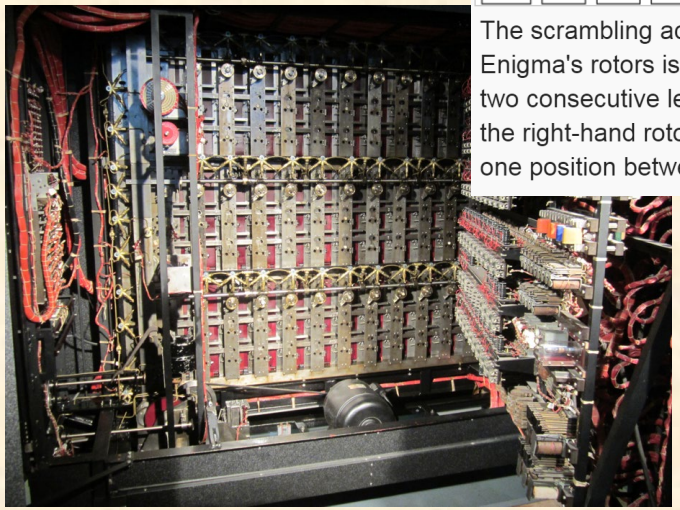


The scrambling action of Enigma's rotors is shown for two consecutive letters with the right-hand rotor moving one position between them.



https://en.wikipedia.org/wiki/Enigma_machine

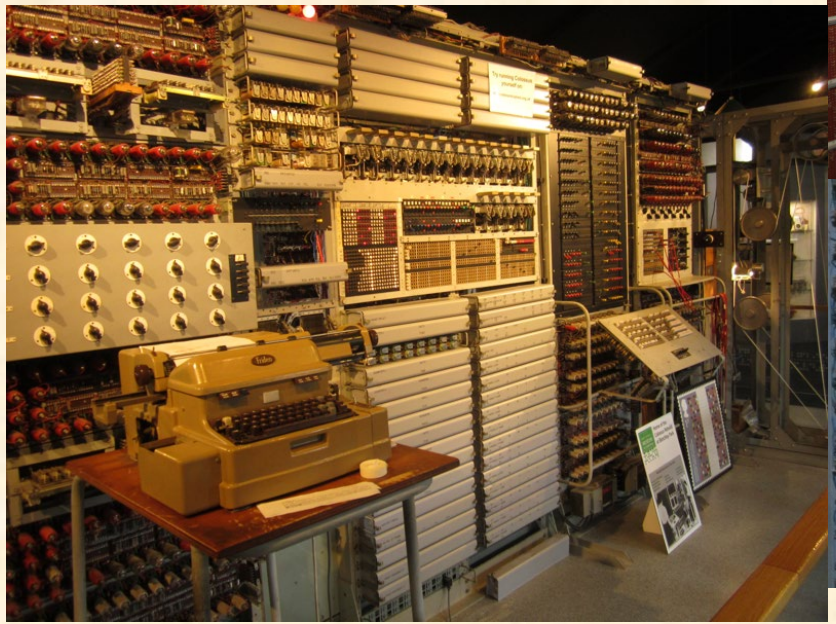


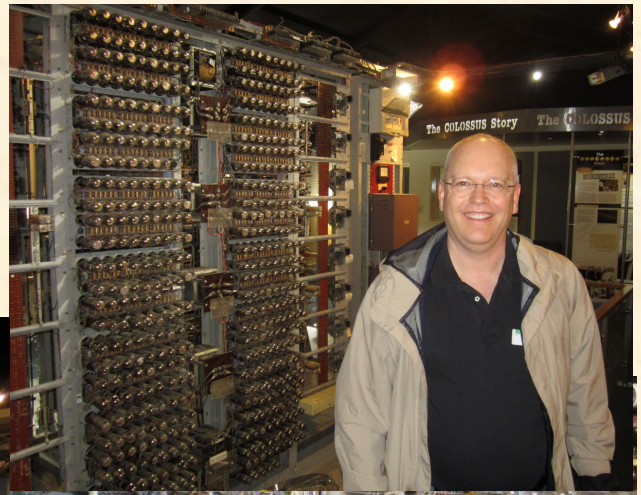


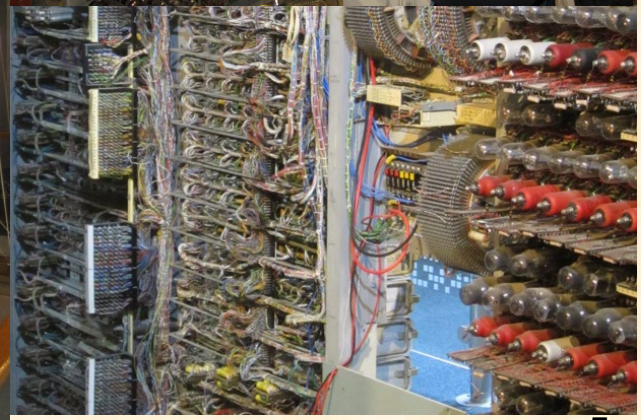
Cryptography Spawned Modern Computers

Carnegie Mellon University

- Colossus: 1943 – 1945
  First stored-program computer
  - Broke German High Command Lorenz cipher
  - Vacuum tube technology
    - Statistical analysis of radio intercepts



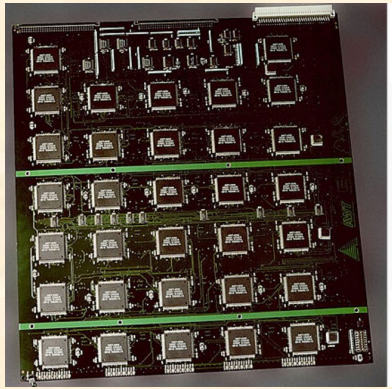




Modern Cryptography

Carnegie Mellon University

- Data Encryption Standard (DES) – 1975
  - Break data to be encrypted into 64-bit blocks
  - 56 bit secret key used to control encryption and decryption
    - Run forward for encryption; run "backward" for decryption
    - Key size (presumably) chosen so "only" NSA could decrypt
      - » (See: NOBUS "NObody BUt Us")
- Publicly broken in 1998
  - $250,000 FPGA hardware
  - Brute force search all 2^{56} DES keys in a few days



The EFF's US$250,000 DES cracking machine contained 1,856 custom chips and could brute force a DES key in a matter of days—the photo shows a DES Cracker circuit board fitted with several Deep Crack chips.

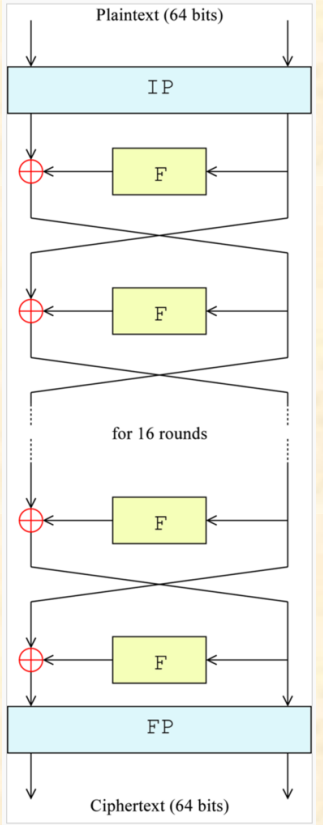
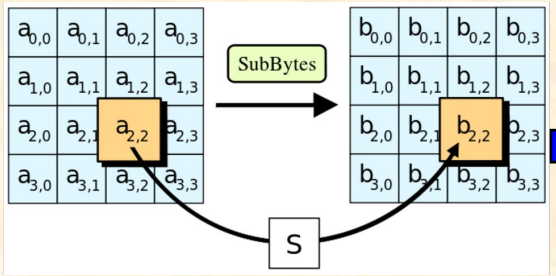


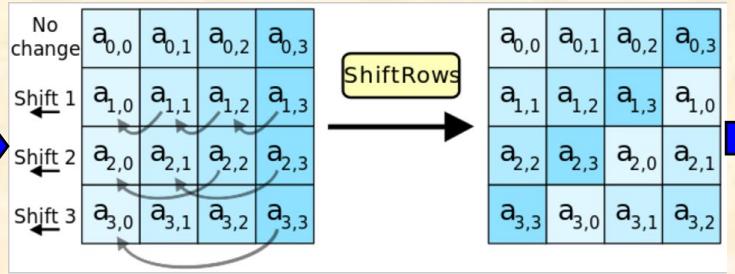
Figure 1— The overall Feistel structure of DES

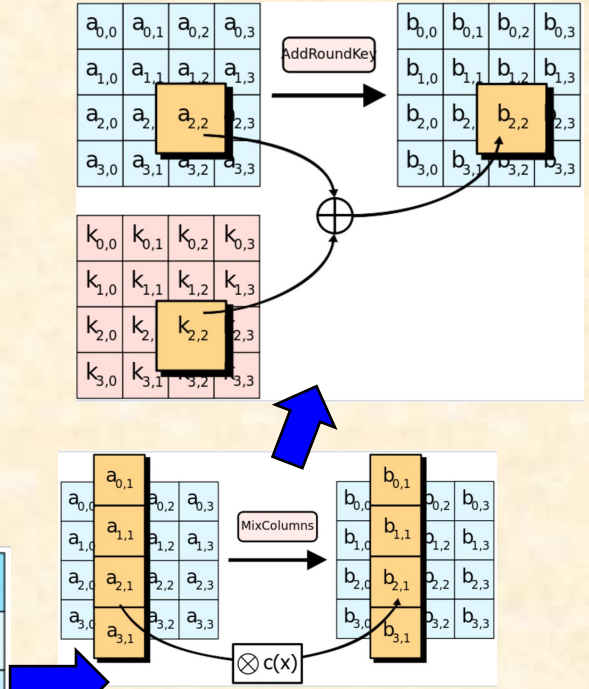
Current-Day Cryptography

Carnegie Mellon University

- Advanced Encryption Standard (AES / Rijdael) – 2001
  - Data to be encrypted into 128-bit blocks
  - Secret key of 128, 192, or 256 bits (e.g., AES-256)
  - Four stages per round:
    - Substitution of byte values: SubBytes
    - Shift rows of bytes: ShiftRows
    - Multiply each column by Matrix: MixColumns
    - XOR with round secret key: AddRoundKey
  - As far as we know, AES is still OK



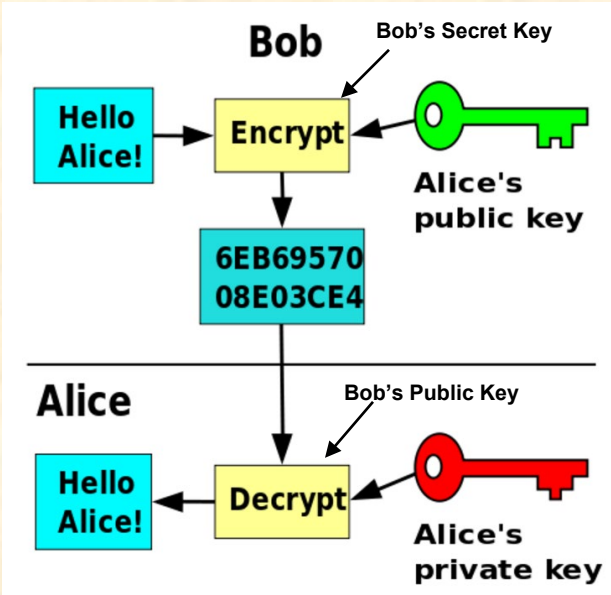




Public Key Cryptography

Carnegie Mellon University

- Previous ciphers were symmetric key
  - Same key used to encrypt and decrypt
- Public key cryptography = asymmetric key pairs
  - Public key: not secret ➔ known to everyone
  - Private key: secret key ➔ known only to key owner
  - Special math relationship for key pairs
    - e.g., PublicKey based on product of two prime numbers
  - Determining secret key given public key is difficult
    - e.g., SecretKey based on prime factors of PublicKey
  - Large key size – 2048 or 3072 bit keys
    - Sparse key space; only need to find a prime factor half that size to break crypto
- Encrypt(BobSecret, AlicePublic) ➔ only Alice can read
  - Alice performs Decrypt(BobPublic, AliceSecret)

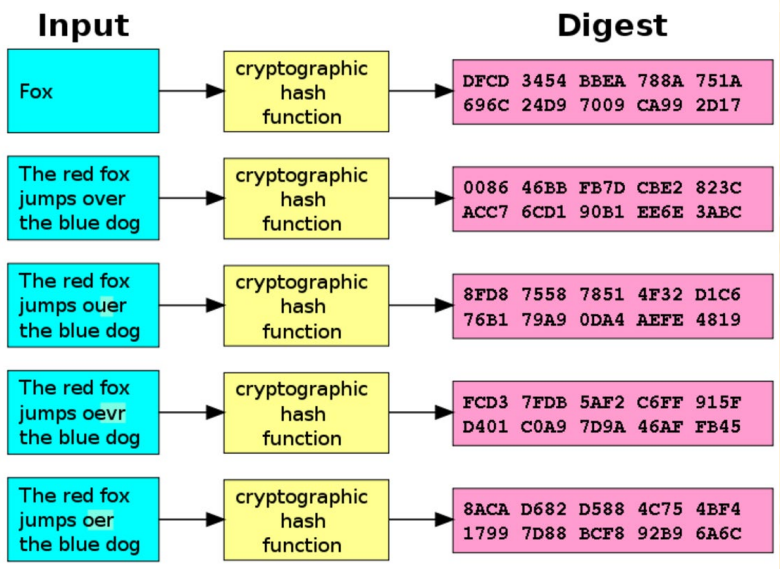


https://en.wikipedia.org/wiki/Public-key_cryptography

Secure Hashing & Digital Signatures

Carnegie Mellon University

- Cryptography can also be used to ensure integrity via creating a digest
  - Non-secure example: checksum/CRC ensures message integrity
  - Advantage: usually a blanket export exemption
- Hashing: Symmetric cryptography
  - Secret key used to create digest of data
  - Same secret key used to check validity
  - Sender & receiver must both have secret key
    - Receiver can forge a signature!
- Signing: Asymmetric cryptography
  - Secret key used to create digest of data
  - Public key used to check validity
  - Receiver cannot forge a signature



A cryptographic hash function (specifically SHA-1) at work. A small change in the input (in the word "over") drastically changes the output (digest). This is the so-called avalanche effect.

https://en.wikipedia.org/wiki/Cryptographic_hash_function

Certificates and PKI

Carnegie Mellon University

- Digital certificate
  - Binds Identity with a Public Key
    - How do you know BobPublicKey is really from Bob?
- Elements of Public Key Infrastructure
  - Certificate Authority
    - Generates asymmetric key pairs
    - Sends you a private key; sends VA your public key
  - Registration Authority
    - Handles personal identification (e.g., checks passport against person) for CA
  - Validation Authority
    - Provides access to Database of {Identity, PublicKey} pairs (digitally signed by CA)
      - » If you know public key of CA, you can check validity of signed {Identity, PublicKey} pairs off-line
    - Handles key revocation if key is compromised (requires on-line access!)

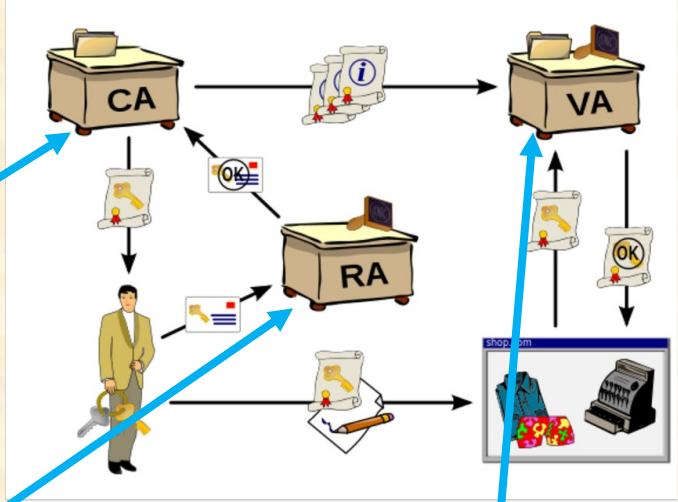


Diagram of a public key infrastructure

https://en.wikipedia.org/wiki/Public_key_infrastructure

Key Material Distribution

Carnegie Mellon University

- Secret keys need to get to each device
  - Each device should have a unique random secret key
    - Also, should have manufacturer public key
  - Ideally:
    - Device SecretKey – to encrypt outgoing messages
    - Device Signed PublicKey – tell factory your public key
      - » (Signed by factory so factory to authenticate it is a legitimate device)
      - » Database of devices will go stale; need device to self-authenticate
    - Factory PublicKey – to receive messages+updates from factory
- Typical encryption use
  - Use public key crypto to exchange symmetric "session key"
  - Use symmetric crypto for actual communications

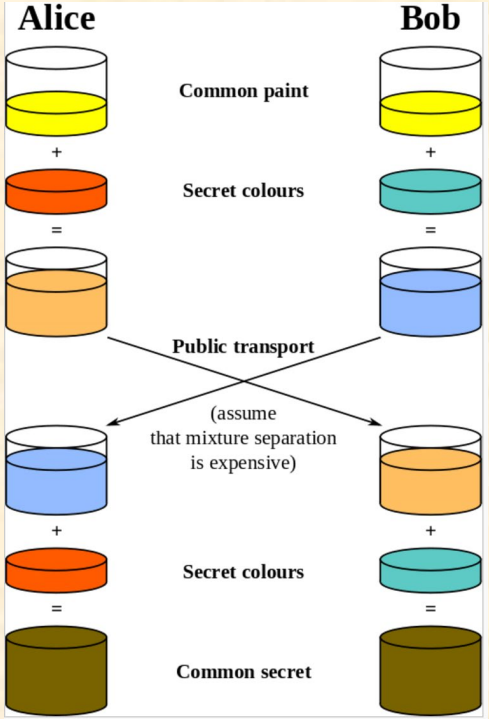
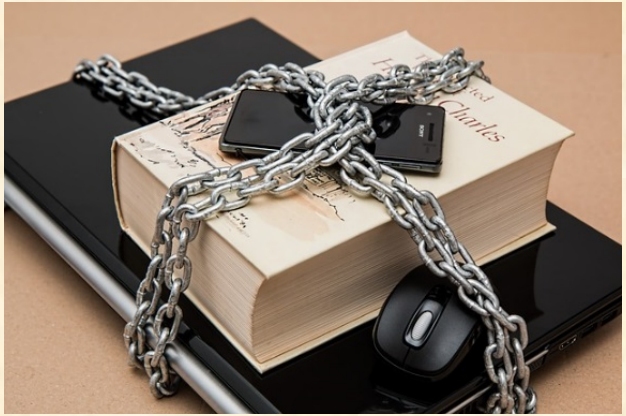


Illustration of the Diffie–Hellman Key Exchange

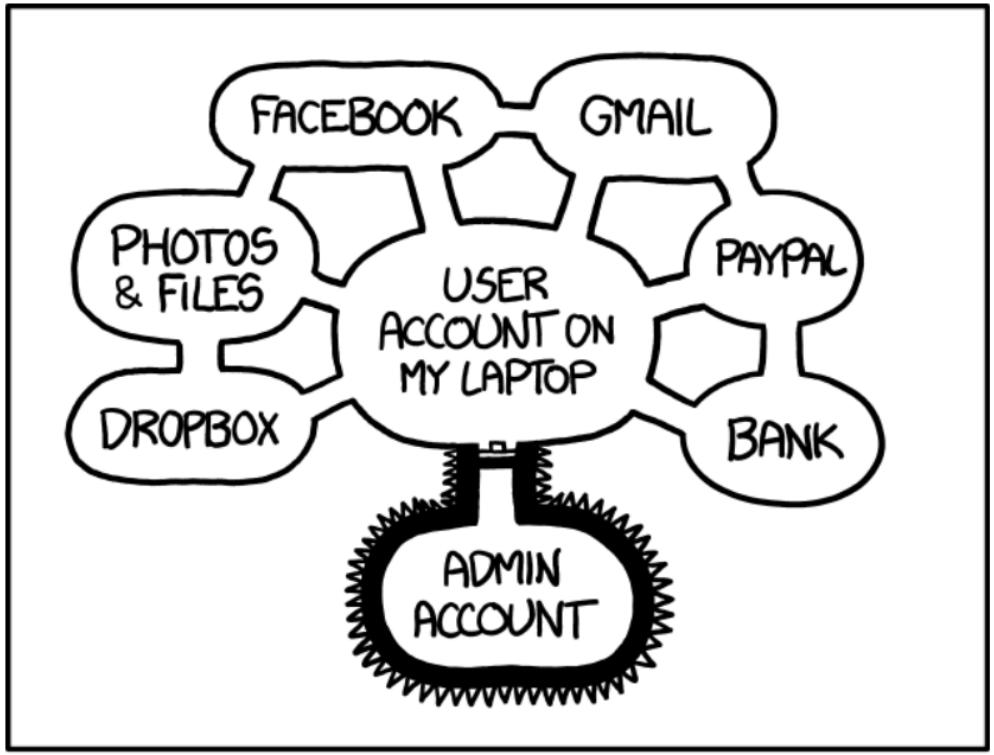
Best Practices For Cryptography

Carnegie Mellon University

- Use well known, standard crypto
  - Private key: faster, but both sides have the key
  - Public key: no sender key in captured receiver
  - Ensure you use a large enough key
    - Deal with key management, including revocation
  - Use hashing/signature when possible



- Pitfalls:
  - Assume that any home-made cryptographic algorithm is insecure
  - How you use encryption is also tricky; don't invent your own protocols
  - Cryptographic algorithms in books can have bugs
    - Get an up-to-date, maintained crypto library from a reputable source



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

https://xkcd.com/1200/