2: Introduction

- 5 Goals
- Symmetric vs Asymmetric

3: Transpositions & Substitutions

- Transposition + examples
- 2 types of Substitution + examples

4: How to Break Transposition & Substitution Ciphers

- Frequency of words and letters
- Bigrams / trigrams / anagramming
- Shannon's principle
- Kasiski method
- Pigeonhole principle

5: Symmetric Cryptography: Classical to Modern

- C = ? P = ?
- One-Time Pad + 2 K constraints
- C = ? P = ?
- Security notion:
    - Attack model (2 models)
    - Security goal (2 goals)
- CPA, CCA, KPA, COA
- Kerckhoffs's Principle

6: Symmetric Cryptography: Block Ciphers

- Block cipher: block size, key size, repetition of rounds
- DES's blocks and AES's blocks bits?
- Lengths are powers of two
- Round key, key schedule algorithm
- DES encoding? C = F3(F2(F1(P))) / P = F'3(F'2(F'1(C)))
- AES encoding? S (C: non-L), P (D: LA, Mat)
- Key-dependent or key-independent?

7: The Advanced Encryption Standard (AES)

- AES (og name Rijndael) is the most-used cipher in the world.
- Before: DES (56-bit keys: too small) / 3DES (168-bit keys to provide 112-bit security).
- Secret key: 128 (most common because it is the fastest), 192, or 256 bits.
- AES manipulates bytes within blocks with 128 bits as a 16-byte 2D array (S means state).
- AES uses a substitution-permutation network with rounds (10 for 128-bit keys, 12 for 192-bit keys, 14 for 256-bit keys)/ Each round (except the last) has 4 steps:
    - SubBytes (substitution): Replaces each byte using a specified S-box
    - ShiftRows (permutation): Shifts the rows using a specified pattern (not the 1st row)
    - MixColumns (permutation): Linear transformation to each of the 4 columns
    - AddRoundKey: XORs a round key to the internal state
- Key schedule in AES: KeyExpansion
- Given any round key, an attacker can determine all other round keys + the main key
- AES Implementations: no production-level AES code with SubBytes() ShiftRows() MixColumns() functions
- Fast AES software: table-based implementations. Vulnerable to cache timing attacks.
- AES native instructions (AES-NI) solve this problem

8: Modes of Operation

- The mode of operation: the biggest danger in using AES
- ECB / CBC / CFB: length of the plaintext VS block size?
    - 2 approaches?
- PKCS#7 for 16-byte blocks:
    - One byte leftover: pad the message with 15 bytes of 0x0f
    - Two bytes leftover: pad with 14 bytes of 0x0e
    - Three bytes leftover, pad with 13 bytes of 0x0d
    - Etc..
    - If the length of the message is already a multiple of 16: add 16 bytes of 0x10
    - Why: allow for the unambiguous removal of the padding after decryption. prioritizes the integrity of the decryption process by eliminating any uncertainty about how to remove the padding. This prevents potential data loss or misinterpretation
- OFB / CTR

9: Stream Ciphers

- What do they do?
- KS = ? C = ? P = ?

- N?
- What should you never do?
- Stateful produce what?
- Counter based produce 2 what? (chunks of keystream from a key, nonce, counter value)
- Hardware-oriented (LFSRs) + example?
- Software-oriented rely on what?+ examples

10: Diffie-Hellman

- asymmetric cryptography does 2 what?
- Diffie-Hellman allows Person A and Person B to generate what?
- forward secrecy?
- Used for HTTPS

11: Public-Key Cryptography

- Asymmetric encryption = public-key encryption
- How many keys? What do they do?
- C = ? P = ?
- Process for public-private keypair?
- Secure if which keys leaks?
- Algorithm example? R,D,ElG, ECC
- What is the hard problem?
- Attack Models & Security Goals (CPA)?

12: Digital Signatures

- A digital signature is what?
- 3 goals of a valid digital signature? (A,I, NR)
- N = ? M = ?
- Who sets the public-private keypair
- Digital Signature Algorithms? ElG, Schorr
- OpenPGP (Pretty Good Privacy)?
- OpenPGP provides 5 features?
- What do you need to set up OpenPGP?
- How do you distribute a public-key?
- Public-Key Infrastructure (PKI)?
- Web of Trust?
- Hash-Then-Sign?
- ‘Sign-then-encrypt’ or ‘encrypt-then-sign’?

- Hybrid Cryptosystems combine what?
- A hybrid cryptosystem is constructed using any 2 separate cryptosystems? (k encap / k sess + d encap)
- Hybrid cryptosystems are used by who?

13: Elliptic Curves

- Elliptic Curve Cryptography (ECC) is an alternative to what?
- Key sizes?
- Power and efficiency VS RSA and classical Diffie-Hellman?
- NIST Recommended Key Sizes?
- Elliptic Curve is based on ECDLP
- RSA is based on what problem? Diffie-Hellman?
- Trapdoor Function? For RSA?
- 3 examples of Elliptic curves for key agreement, digital signatures and public-key encryption?
- An elliptic curve equation? y2 = x3 + ax + b
- How to choose a and b?

14: Hashing

- Hash Functions examples?
- Used for what?
- A hash function does what? M > HF > H (256, 512)
- Cryptographic hash functions are resistant to what?
- Hash(M) = H
- P resistance? 2 types?
- Collision resistance? Bird + happy?
- Avalanche effect?
- The cryptographic strength of hash functions?
- Building Hash Functions: 2 types
- Iterative hashing (chunks)? 2 types?
- Compression-Based Hash Functions (blocks)?
- Permutation-Based Hash Functions (XOR, newer)?
- Popular Hash Functions?

15: Keyed Hashing

- Keyed Hash Functions VS non-keyed hash? K+M > HF > H
- Keyed hashing forms the basis of two types of important cryptographic algorithms?
- Message Authentication Codes (MACs)? Integrity, auth > Auth tag? T = MAC(K, M)
- Pseudorandom Functions (PRF)? PRF(K, M)? KDerivationF and PBKDF? Identification schemes?

- Popular Keyed Hash Functions? HMAC-*, *-CMAC, SipHash

16: Applications of Hashing

- Verifying the Integrity of Messages? chain of trust? CRC?
- Signature Creation & Verification? Size advantage?
- The security in bits for a hash function is half the size of the hash due to the birthday attack: weakest link?
- Passphrase Storage & Verification: don't do what? BEST OPTION?
- Popular Iterated Hash Functions? Bcrypt, scrypt, argon2
- Time–memory trade-off?
- Scrypt?
- The minimum memory required to compute the function is 128 * N * r bytes
- File & Data Identification: Git and Magnet use SHA-1 hashes
- Proof-of-Work?

17: Merkle Trees

- Hash function
- Merkle tree
- Merkle proof

18: Quantum Cryptography

- Quantum Superposition
- Quantum Entanglement
- Quantum Tunneling
- Heisenberg Uncertainty Principle
- Initial State Preparation
- Quantum Circuit / Algorithm Execution
- Quantum Speedup
- Shor's Algorithm
- Grover's algorithm (quadratic speedup)
- Post-Quantum Cryptography
- Code-Based Cryptography
  - Lattice-Based Cryptography
  - Multivariate Cryptography
  - Hash-Based Cryptography
- Candidate PQC Algorithms:
  - (CRYSTALS-)Kyber
  - (CRYSTALS-)Dilithium

- Falcon
- SPHINCS+