Cryptography

Intro to Crypto

By Alkalem, modified by Hanna3-14, modified again by uxxct

04.12.2025

Why?

Security Goals

- **Confidentiality:** Protecting personal data
- **Integrity:** Data has not been modified
- **Authenticity:** Exactly what is claimed

Classical Cryptography

Caesar cipher

- Each letter is shifted by a fixed value K
- $encrypt_K(P) = (P + K)\ mod\ 26$
- $decrypt_K(C) = (C - K)\ mod\ 26$

Example for K = 23:

Plaintext:	T	H	E		Q	U	I	C	K		B	R	O	W	N		F	O	X	...
Ciphertext:	Q	E	B		N	R	F	Z	H		Y	O	L	T	K		C	L	U	...

Classical Cryptography

Vigenère cipher

- Choose a key of multiple letters, shift each letter according to the key letter
- Attacks: Determine key length, frequency analysis, (Kasiski examination)

Example:

Plaintext:	A	T	T	A	C	K	A	T	D	A	W	N
Key:	L	E	M	O	N	L	E	M	O	N	L	E
Ciphertext:	L	X	F	O	P	V	E	F	R	N	H	R

Classical Cryptography

One Time Pad (OTP)

- Use key with same length as plaintext
- **Information-theoretically secure,** if key is chosen equally distributed at random and used only once
- Key exchange needs to be done separately via a secure channel
- Mostly not realizable

Randomness

- In most programming languages default pseudo-random number generators (PRNGs) are not cryptographically secure

  ⇒ State can be recovered

- Cryptographically Secure RNGs:
  - getrandom
  - Hardware RNGs
  - RNGs of the cryptographic libraries (e.g., secrets or Crypto.Random in python)

Symmetric Cryptography

Stream Ciphers

- Pseudo-random key stream generated from key with an PRNG
- Key stream is XORed with plaintext stream
- Examples: RC4, SEAL, Salsa, CryptMT
- Attacks:
  - Known Plaintext: Calculate parts of the key stream when parts of plaintext are known
  - Key Reuse: Two messages are encrypted with same key stream, difference (XOR) between plaintexts is observable

Symmetric Cryptography

Block Ciphers

- Encrypt blocks of fixed length
- Padding: Extend messages to full block length
- Examples: DES, IDEA, RC5, AES, Blowfish, ...
- Modes Of Operation: (e.g. ECB, CBC, CTR, GCM)
- Attacks:
  - Against Cipher: Differential or linear cryptanalysis
  - Different Attacks against different modes of operation

RSA - Key Generation

- Choose large prime numbers p and q
- Calculate the modulus $N = p * q$
- Calculate $\phi(N) = (p-1) * (q-1)$
- Choose e with $gcd(e,\ \phi(N)) = 1 \land 1 < e < \phi(N)$
- Calculate d as inverse of e under modulus $\phi(N)$

$$e * d \equiv 1 \mod \phi(N)$$

- Public Key: $N,\ e$
- Private Key: d

RSA - Encryption and Decryption

- Encryption: $c = m^e \mod N$
- Decryption: $c^d = (m^e)^d = m^{ed} \mod \phi(N) = m^1 \mod N$
- RSA without special padding is homomorphic ($Enc(m_1, pk) * Enc(m_2, pk) = Enc(m_1 * m_2, pk)$) and deterministic
- Use RSA-OAEP if that is problematic

RSA - Attacks

- Factoring N is infeasible for reasonable choice of N
- In some cases, attacks in polynomial time possible:
  - Small private exponent d ($d < \frac{1}{3}N^{\frac{1}{4}}$): Wiener's attack
  - For small public exponent or partially known prime factor: Coppersmith's attack
  - $m < N^{\frac{1}{e}}$: calculate message as root of ciphertext
  - Message sent to many recipients using same public exponent: Hastad's Broadcast Attack

Elliptic Curves

- Elliptic Curve Equation:
- Group: Generator point G, point addition and multiplication with natural number
- Cyclic EC group over $\mathbb{Z}_p, p > 3$
- Point (x, y) on curve iff $y^2 \equiv x^3 + ax + b \mod p$, plus (imaginary) point at infinity O, $a, b \in \mathbb{Z}_p$ with $4a^3 + 27b^2 \not\equiv 0 \mod p$
- Harder to attack, can use smaller keys for same security level

ECC - Common Problems

- Bad curves or parameters
- Bad (P)RNG
- Nonce reuse

Typical Cryptography Vulnerabilities

- Implementation Mistake: Incorrect/vulnerable custom implementation, incorporated incorrectly into application
- Conceptual Mistake: Incorrect use or not sufficient for use case
- Theoretic Mistake: Violated condition for security, advanced maths or theoretic computer science necessary, "read the paper"
- Well-known and documented attacks (e.g. length extension attack)
- Oracles

Tools

- CyberChef
- https://factordb.com/
- sagemath (free open-source mathematics software system)
- Z3 (theorem prover)

Further Topics

- Post-Quantum Cryptography
- Pairing-Based Cryptography
- Zero Knowledge

Start Playing Crypto CTF

- https://intro.kitctf.de/
- Other Platforms:
  - https://cryptohack.org/ (Easy to hard, with good explanations)
  - https://cryptopals.com/ (Implement cryptosystems and attacks)
  - https://overthewire.org/wargames/krypton (Classical crypto)
  - https://imaginaryctf.org/ (Not only crypto but also other CTF challenges)