Introduction to Cryptography

Alvin Lin

January 2018 - May 2018

Cryptography

Desired security properties in the digital world:

- confidentiality, secrecy
- data integrity
- authentication, of data origin and entity
- non-repudiation

Cryptography is an important, but only a relatively small part of security:

- the right choice of tools is hard
- implementation errors are common
- a variety of side-channel attacks can bypass the best cryptography
- social engineering

Unkeyed, Symmetric-Key, and Public-Key

Primitives, algorithms, and protocols can be **unkeyed**, **symmetric-key**, or **public-key**.

Unkeyed

This includes hashing and the SHA-family of algorithms. It can be used for signing and the generation of random sequences.

Symmetric Keys

All encryption schemes from ancient times until 1976 were symmetric ones. The same key is used for both encryption and decryption. Encryption and decryption are inverse operations if the same key is used on both sides. Keys must be transmitted via some other secure channel.

- Block ciphers since the 1970s: IBM's Lucifer, DES (Data Encryption Standard), IDEA (International Data Encryption Standard), AES (Advanced Encryption Standard).
- Stream ciphers: RC4, also can come from counter mode of block ciphers or hash functions.
- MAC, HMAC: message authentication codes.
- PRNG: pseudorandom number generators

Public Key (Asymmetric)

- Public-key cryptosystems: RSA (Rivest, Shamir, Adleman), ElGamal, McEliece cryptosystems, ECC (elliptic curve cryptosystems).
- Signatures: DSS/DSA (Digital Signature Standard/Algorithm), ECDSA (Elliptic Curve Digital Signature Algorithm).
- PKI: public key infrastructure, DH (Diffie Hellman key agreement), key management, and distribution.
- Homomorphic cryptography: Paillier, Gentry

Main Public-Key Systems in Use

RSA by Rivest-Shamir-Adleman (1977) has an edge of ECC because:

- it is simple and well understood
- links nicely to basic number theory
- deployed earlier on many systems

ECC by Koblitz-Miller (1985) has an edge over RSA because:

- it uses short keys (163+ bits vs 1024+ bits for RSA)
- delivers much better performance
- uses great theory of elliptic curves on top of classical number theory used by RSA

Other composite and special functionalities

- Zero-knowledge protocols
- Authenticated encryption CAESAR competition
- Electronic cash: untraceable, no double-spending, bank-shop-customer roles, central banks
- Cryptocurrencies: Bitcoin, Zerocoin, Litecoin, Darkcoin, etc
- Electronic voting: no individual vote auditing
- Oblivious transfer: two millionaires problem
- Quantum and post-quantum cryptography, quantum key distribution, quantum computing

The majority of today's protocols are hybrid schemes. We use symmetric ciphers for encryption and message authentication, and asymmetric ciphers for key exchange and digital signatures.

Why do we need Cryptanalysis?

There is no mathematical proof of security for any practical cipher. The only way to have assurance that a cipher is secure is to try to break it (and fail). **Kerckhoff's Principle** is paramount in modern cryptography: A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In order to use Kerckhoff's Principle in practice, only use widely known ciphers that have been cryptanalyzed for several years by good cryptographers.

It is tempting to assume that a cipher is "more secure" if its details are kept secret. However, history has shown time and again that secret ciphers can almost always be broken once they have been reverse engineered.

Cryptanalysis: Attacking Cryptosystems

Classical attacks involve mathematical analysis or brute-force attacks. Implementation attacks try to extract the key through reverse engineering and various side-channel attacks. Social engineering attacks try to trick users into giving up passwords and authentication details.

> You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech