CO 487 Applied Cryptography

Keven Qiu
Instructor: Alfred Menezes
Winter 2024

Chapter 1

Introduction

Definition: Cryptography

Securing communications in the presence of malicious adversaries.

Fundamental goals of cryptography:

- Confidentiality: keep data secret from all but those authorized to see it.
- Data integrity: ensuring data has not been altered by unauthorized means.
- Data origin authentication: corroborating the source of data.
- Non-repudiation: preventing an entity from denying previous commitments or actions.

Definition: Transport Layer Security (TLS)

The cryptographic protocol used by web browsers to securely communicate with websites.

Used to assure an individual user (client) of the authenticity of the website (server) they are visiting, and to establish a secure communications channel for the remainder of the session.

Definition: Symmetric-Key Cryptography

The client and server a priori share some secret information k called a key.

They can engage in secure communication by encrypting with AES and authenticate the resulting ciphertexts with HMAC.

Definition: 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.

Definition: Signature Scheme

The 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.

Chapter 2

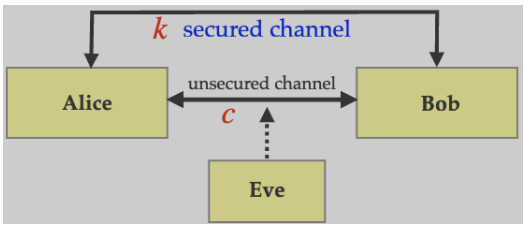
Symmetric-Key Encryption

Definition: Symmetric-Key Encryption Scheme (SKES)

Consists of

- M: the plaintext space
- C: the ciphertext space
- K: the key space
- A family of encryption functions $E_k : M \to C$ for all $k \in K$
- A family of decryption functions $D_k : C \to M$ for all $k \in K$

such that $D_k(E_k(m)) = m$ for all $m \in M, k \in K$.



Alice and Bob agree on a secret key $k \in K$ by communicating over the secured channel. Alice computes $c = E_k(m)$ and sends the ciphertext c to Bob over the unsecured channel. Bob retrieves the plaintext by computing $m = D_k(c)$.

A substitution cipher is a simple symmetric-key encryption scheme.

Definition: Security Model

Defines the computational abilities of the adversary and how she interacts with the communicating parties.

Definition: Convention

Always strive to model maximal adversary capabilities and minimal adversary goals.

Basic assumption: The adversary knows everything about the SKES, except the particular key k chosen by Alice and Bob.

Definition: Information-Theoretic Security

Eve has infinite computational resources.

Definition: Complexity-Theoretic Security

Even has a polynomial-time Turing machine.

Definition: Computational Security

Eve is computationally bounded by resources.

2.1 Adversary's Interaction

2.1.1 Passive Attacks

Definition: Ciphertext-Only Attack

The adversary knows some ciphertext.

Definition: Known-Plaintext Attack

The adversary knows some plaintext and the corresponding ciphertext.

2.1.2 Active Attacks

Definition: Chosen-Plaintext Attack

The adversary can choose some plaintext and obtains the corresponding ciphertext.

Definition: Clandestine Attack

Bribery, blackmail, etc.

Definition: Side-Channel Attack

Monitor the encryption and decryption equipment.

2.2 Adversary's Goal

1. Recover the secret key k.
2. Systematically recover plaintext from ciphertext, without necessarily learning k.
3. Learn some partial information about the plaintext from the ciphertext, other than its length.

Definition: Totally Insecure

The SKES is totally insecure if the adversary can achieve 1 or 2.

Definition: Semantically Secure

The SKES is semantically secure if the adversary cannot learn any partial information about the plaintext from the ciphertext (except possibly length).

Definition: Secure SKES

A symmetric-key encryption scheme is said to be secure if it is semantically secure against chosen-plaintext attack by a computationally bounded adversary.

To break a SKES, the adversary has to accomplish the following:

1. The adversary is given a challenge ciphertext c.
2. During its computation, the adversary can select plaintext and obtain the corresponding ciphertext.
3. After a feasible amount of computation, the adversary obtains some information about the plaintext m corresponding to c.

Desirable properties of a SKES:

1. Efficient algorithms should be known for computing E_k and D_k.
2. Secret key k should be small, but large enough to render exhaustive key search infeasible.
3. Scheme should be secure, even against the designer of the system.

The simple substitution cipher is totally insecure against a chosen-plaintext attack.

There are $26! \approx 2^{88}$ keys to try.

Work Factor:

- 2^{40} operations is considered very easy.
- 2^{56} operations is considered easy.
- 2^{64} operations is considered feasible.
- 2^{80} operations is considered barely feasible.
- 2^{128} operations is considered infeasible.

Definition: Security Level

A cryptographic scheme is said to have a security level of ℓ bits if the fastest known attack on the scheme takes approximately 2^{ℓ} operations.

2.3 Polyalphabetic Ciphers

Idea: Use several permutations, so a plaintext letter is encrypted to one of sever possible ciphertext letters.

Vigenere Cipher: The secret key is an English word having no repeated letters, e.g. $k =$ CRYPTO.

Example: if $m =$ "this is a message", and $k =$ "CRYP TO C RYPTOCR", then $c =$ "VYGH BG C DCHLOIV". Here $A = 0, \ldots, Z = 25$ and addition of letters is modulo 26.

Decryption is subtraction modulo 26: $m = c - k$. The frequency distribution of ciphertext letters is flatter than for a simple substitution cipher.

The Vigenere cipher is totally insecure against a chosen-plaintext attack and totally insecure against ciphertext-only attacks.

2.4 One-Time Pad

The secret key is a random string of letters. The key should not be reused:

- If $c_1 = m_1 + k$ and $c_2 = m_2 + k$, then $c_1 - c_2 = (m_1 + k) - (m_2 + k) = m_1 - m_2$.
- So, $c_1 - c_2$ depends only on the plaintext, not the key k, and hence can leak information about the plaintext m_1 and m_2.

2.4.1 Binary Messages

By convention, we will assume messages and keys are binary strings. $\oplus$ denotes exclusive-or, i.e. bitwise addition mod 2.

- $x \oplus x = 0$
- $x \oplus y = y \oplus x$
- If $x = y \oplus z$, then $x \oplus y = z$

So for the one-time pad, encryption is $c = m \oplus k$ and decryption is $m = c \oplus k$.

2.4.2 Security of One-Time Pad

Definition: Perfect Secrecy

The one-time pad is semantically secure against ciphertext-only attack by an adversary with infinite computational resources.

Shannon proved that if plaintexts are ℓ-bit strings, then any symmetric-key encryption scheme with perfect secrecy must have $|K| \geq 2^{\ell}$.

2.5 Stream Ciphers

Basic idea: Instead of using a random key, use a pseudorandom key.

Definition: Psuedorandom Bit Generator (PRBG)

A deterministic algorithm that takes as input a random seed, and outputs a longer pseudorandom sequence called the keystream.

Definition: Stream Cipher

Uses a PRBG for encryption and the seed is the secret key shared by Alice and Bob.

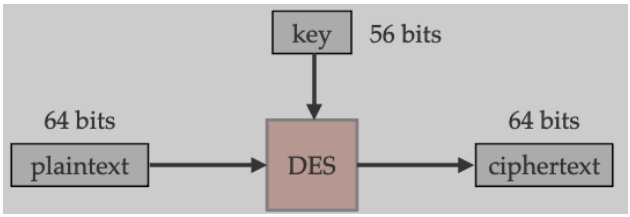
Indistinguishability Requirement: The keystream should be indistinguishable from a random sequence.

Unpredictability Requirement: Given portions of the keystream, it should be computationally infeasible to learn any information about the remainder of the keystream.

If an adversary knows a portion c_1 of ciphertext and the corresponding plaintext m_1, then she can easily find the corresponding portion $k_1 = c_1 \oplus m_1$ of the keystream.

2.5.1 ChaCha20

Uses only simple arithmetic operations: integer addition modulo 2^{32}, xor, and left rotations.



Notation: 256-bit key $k = (k_1, \ldots, k_8)$, 96-bit nonce $n = (n_1, n_2, n_3)$, 128-bit constant $f = (f_1, \ldots, f_4)$, 32-bit counter c. The initial state is

$$\begin{bmatrix} f_1 & f_2 & f_3 & f_4 \\ k_1 & k_2 & k_3 & k_4 \\ k_5 & k_6 & k_7 & k_8 \\ c & n_1 & n_2 & n_3 \end{bmatrix} = \begin{bmatrix} S_1 & S_2 & S_3 & S_4 \\ S_5 & S_6 & S_7 & S_8 \\ S_9 & S_{10} & S_{11} & S_{12} \\ S_{13} & S_{14} & S_{15} & S_{16} \end{bmatrix}$$

A hexadecimal digit is a 4-bit number. A nonce (or initializing value) is a non-repeating quantity.

$\oplus$ is xor, $\boxplus$ is integer addition mod 2^{32}, $<<< t$ is left-rotation by t positions. The Quarter Round function takes in four 32-bit words and outputs these words after mixing some bits.

There is a ChaCha20 keystream generator. To encrypt, the keystream bytes are xored with the plaintext bytes to produce ciphertext bytes. The nonce is appended to the ciphertext.

2.6 Block Ciphers

Definition: Block Cipher

A symmetric-key encryption scheme that breaks up the plaintext into blocks of fixed length (e.g. 128 bits) and encrypts the blocks one at a time.

Stream ciphers usually encrypt one bit a time.

The key length is 56 bits, size of key space is 2^{56}, and the block length is 64 bits.