1 Introduction to Security

1.1 Objectives

1.1.1 Confidentiality

1.1.2 Data Integrity

1.1.3 System Integrity

1.1.4 Availability

1.1.5 Non-Repudiation

1.1.6 Authenticity

1.1.7 Privacy

1.2 Attacker Modeling Principles

1.2.1 Safe Assumptions

1.2.2 Attacker Capabilities and Knowledge

1.2.3 Rejection of Security by Obscurity

2 Introduction to Cryptography

3 Stream Ciphers

4 Block Ciphers

5 Block Cipher Modes of Operation

6 Public-Key Encryption

7 Hash Functions

8 Message Authentication

9 Digital Signatuers

10 Key Distribution

11 Public-Key Distribution

Glossary

accountability actions can be provably traced back to an entity

Advanced Encryption Standard encryption standard consisting of invertible rounds in which a different key is generated each round

affine cipher cipher $E(x) = (ax + b) \bmod m$

asymmetric-key cryptography see public-key cryptography

attacker model what the attacker can do, what they know, and what they want to achieve

authenticated encryption encryption system that provides both confidentiality and integrity

authenticity information comes from verified and trusted sources (e.g., user authentication)

availability information and system functionality is available to authorized entities

birthday attack for an m-bit hash, trying $\sqrt{2^m} = 2^{m/2}$ inputs until a collision is found

birthday paradox probability that two people share a birthday in a group of N is

$$\prod_{i=1}^{N-1} \frac{365 - i}{365} \approx e^{-\frac{N^2}{730}}$$

which is approximately 0.5 at $N = 23$. More generally, if we sample N values from a set of M elements, a collision is likely if $N > \sqrt{M}$

block cipher a cipher in which plaintext is encrypted in fixed-size blocks and decryption is a different operation than encryption

block cipher mode of operation technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application

brute-force attack attack model in which every possible key is tried on a given ciphertext until the original plaintext is recovered

caesar cipher a cipher in which each letter of the plaintext is replaced by a letter some fixed number of positions down the alphabet

CBC-MAC MAC based on Cipher Block Chaining (CBC) mode of operation; uses different keys for CBC encryption and CBC-MAC auth; not secure for variable-length messages

ChaCha20 more secure and efficient variant of Salsa20

chosen ciphertext attack attack model in which one or more *chosen* plaintext-cipher pairs is known

chosen plaintext attack attack model in which the attacker can obtain the ciphertext for any plaintext

chosen text attack attack model in which the attacker can obtain the ciphertext for any plaintext *and* one or more chosen plaintext-cipher pairs is known

Cipher Block Chaining Block-oriented Block Cipher Mode that allows for parallel decryption (but not encryption) of blocks and hides patterns in the plaintext. Possible for attacker to rearrange or remove blocks from the ciphertext or tamper with bits of the plaintext and IV must have integrity protection. Application — general-purpose block-oriented transmission

Cipher Feedback Stream-oriented Block Cipher Mode with self-synchronizing stream cipher in which blocks can be decrypted (but not encrypted) in parallel. Attacker can potentially tamper with bits of the plaintext or rearrange or remove blocks. Application — general-purpose stream-oriented transmission

cipher-based MAC MAC that thwarts forgery for variable-length messages

ciphertext only attack attack model in which only the algorithms used and the ciphertext are known

collision resistance see strong collision resistance

computersecurity protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

confidentiality information is not available to unauthorized entities

confusion each bit of the ciphertext should depend on many bits of the key

content modification communication channel attack in which the content of a message is changed

Counter Mode Stream-oriented Block Cipher Mode in which blocks can be encrypted and decrypted in parallel, pre-computation is possible, and bit errors do not propagate. Attacker can potentially tamper with the bits of the plaintext. Application — general-purpose transmission

counter with CBC-MAC encryption based on Counter Mode (CTR); authentication based on CBC-MAC; authenticate, then encrypt

cryptanalytic attack attack model in which the attacker relies on the nature of the algorithm and knowledge of the general characteristics of the plaintext

cryptographic hash function pseudorandom, efficient, collision-resistant, one-way function that maps a variable-length input to a fixed-length hash value

Data Encryption Standard federally approved encryption standard consisting of iterated substitution-permutation cipher of 16 rounds with 64-bit block size and 56-bit key size

data integrity information cannot be modified in an unauthorized and undetected way

denial of service attack against availability

diffusion each plaintext bit should affect the value of many ciphertext bits

digital signature a mathematical scheme to provide both message authenticity and non-repudiation/accountability

digital signature algorithm NIST algorithm designed for signature; cannot be used for encryption; efficient variant of ElGamal Encryption with much smaller signatures and modular arithmetic operations with smaller moduli

digital signature standard Federal Information Processing Standard (FIPS) 186, introducted in 1993; latest version includes RSA, DSA, elliptic-curve signatures

Double DES DES utilizing 2 56-bits. Effective security is only 80-bits

Electronic Code Book Block-oriented Block Cipher Mode that allows for parallel encryption and decryption of blocks, but in which identical plaintext blocks result in identical ciphertext blocks and allows for attackers to rearrange or remove blocks from ciphertext. Application — secure transmission of a single block

ElGamal Encryption encryption scheme which depends on the difficulty of computing discrete logarithms

Elliptic Curve Cryptography approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields

elliptic curve digital signature algorithm signature algorithm based on elliptic curve cryptography with shorter keys and increased efficiency

Galois/Counter Mode encryption based on Counter Mode (CTR); authentication – $\text{GHASH}_H(X)$ takes hash key H and 128-bit message blocks $X = X_1, X_2, \ldots, X_m$ and outputs

$$(X_1 \cdot H^m) \oplus (X_2 \cdot H^{m-1}) \oplus \cdots \oplus (X_{m-1} \cdot H^2) \oplus (X_m \cdot H)$$

hash-based MAC MAC that uses a hash function; provably secure if the hash is pseudorandom; more efficient with iterative hash function; used in IPSsec and SSL/TLS protocols

hash-then-sign sign a cryptographic hash of the message; compatibile with most public-key encryption algorithms, efficient, and prevents existential forgery

integrity information and system functionality cannot be altered by unauthorized entities

iterative hash function hash in which the input is divided into fixed-length blocks and each block is hashed

Kerckhoffs's Principle principle that a cryptographic system should be secure, even if all of its details, except for the key, are publicly known

key-reuse problem security flaw in which attacker can decipher plaintext given multiple ciphertexts encrypted with the same key

known plaintext attack attack model in which one or more plaintext-cipher pairs is known

masquerade communication channel attack in which messages from a fraudulent source are inserted

MD5 Message-Digest Algorithm hash function based on Merkle-Damgård Construction consisting of four rounds, each consisting of 16 operations, with 512-bit block length and 128-bit hash length; not collision resistant – can be broken in $2^{18} = 262144$ steps, less than a second on an average computer

meet-in-the-middle attack a known plaintext attack in which stores intermediate values from encryptions and decryptions to reduce the time necessary to brute-force the decryption keys, effectively trading off time for storage

Merkle-Damgård Construction general method for building a cryptographic hash function from a collision-resistant, one-way compression function; collision-resistant with sufficiently long padding

message authentication code takes a secret key K and an arbitrary-length input M and produces tag T

non-cryptographic hash function computationally inexpensive but generally insecure hash function that can be used for error detection and error correction

non-repudiation see accountability

nonce number used once

one-time pad perfect security in which a single-use encryption key at least as long as the plaintext is chosen randomly and used to encrypt only a single message

one-way property given a hash value h, it is computationally infeasible to find an input y such that $H(y) = h$

Output Feedback Stream-oriented Block Cipher Mode in which bit errors do not propagate and pre-computation is possible, but blocks cannot be encrypted or decrypted in parallel and attacker can tamper with bits of the plaintext. Application — stream-oriented transmission over noisy channel

perfect security attacker gains no information about the plaintext from observing the ciphertext, formally,

$$\mathbb{P}(P = p) = \mathbb{P}(P = p \mid E(K, P) = c)$$

i.e., that the plaintext and ciphertext are independent

PKCS #1 an RSA signature published by RSA Laboratories republished as RFC 3447; older standard of RSASSA-PKCS1-v1_5

preimage resistance see one-way property

privacy assures that individuals have control or influence over information related to them

pseudorandom number generator takes fixed-length seed and generates a sequence of bits using a deterministic algorithm

public-key cryptography using a pair of keys – one private and one public

RC4 (Rivest Cipher 4) stream cipher with variable key length and which uses byte-oriented operations. No longer in use

RSA Cryptosystem encryption scheme which depends on the difficulty of factoring large numbers

RSA signature apply RSA encryption to the hash of the message and send both the encrypted message and hash — receiver decrypts message with public key and applies same hash function and verifies the the hash is the same; commonly used with SHA-256

RSASSA-PSS probabilistic signature scheme (PSS) form of RSA encryption which adds a salt; provably secure assuming RSA is secure

Salsa20 fixed-length key stream cipher that uses 32-bit operations and which can seek to any position in output sequence. 64-bit nonce is part of the algorithm to mitigate key-reuse problem

salt randomized padding added to a message

second preimage resistance see weak collision resistance

secure block cipher a block cipher that is indistinguishable from a random permutation of the blocks (for a computationally bounded attacker)

security by obscurity providing security by keeping the design or implementation of a system secret

security through minority providing security by using software products that are not widely adopted

sequence modification communication channel attack in which the sequence of messages is changed, including potential deletion of messages

SHA-1 160-bit hash with Merkle-Damgård Construction; collision can be found in 2^{65} steps

SHA-2 family of functions: SHA-224, 256, 384, and 512, producing 224, 256, 384, and 512-bit ouputs, respectively; same underlying structure and operations as SHA-1; some weaknesses have been found

SHA-3 hash function to replace SHA-2, uses Sponge Construction; output length can be arbitrary

Sponge Construction hash function that can take an input stream of arbitrary length and return an output stream of any desired length; data is "absorbed" into the sponge and the result is "squeezed" out

stream cipher takes fixed-length seed and uses a pseudorandom number generator to produce sequence of bits as long as the plaintext then encrypts with XOR

strong collision resistance it is computationally infeasible to find any pair of inputs (x, y) such that $x \neq y$ but $H(x) = H(y)$; implies weak collision resistance

substitution cipher permutation over the alphabet

system integrity system performs its intended function

timing modification communication channel attack in which messages are delayed or repeated

Triple DES DES utilizing 3 56-bit keys. Effective security is only 112-bits

weak collision resistance given input x, it is computationally infeasible to find y such that $x \neq y$ but $H(x) = H(y)$

weakest link principle that the attacker needs to find only a single vulnerability

Acronyms

2DES Double DES

3DES Triple DES

AES Advanced Encryption Standard

CBC Cipher Block Chaining

CCA chosen ciphertext attack

CCM counter with CBC-MAC

CFB Cipher Feedback

CIA confidentiality, integrity, and availability

CMAC cipher-based MAC

COA ciphertext only attack

CPA chosen plaintext attack

CTR Counter Mode

DES Data Encryption Standard

DoS denial of service

DSA digital signature algorithm

ECB Electronic Code Book

ECDSA elliptic curve digital signature algorithm

FIPS Federal Information Processing Standard

HMAC hash-based MAC

KPA known plaintext attack

MAC message authentication code

MD5 MD5 Message-Digest Algorithm

OFB Output Feedback

PRNG pseudorandom number generator

PSS probabilistic signature scheme

RSA Rivest, Shamir, Adleman RSA Cryptosystem

SHA Secure Hash Algorithm SHA-1, SHA-2, SHA-3