COMPUTER SECURITY

CHAPTER 4 & 5: CRYPTOGRAPHY

BY : DR. ALA BERZINJI

WHAT IS CRYPTO…?

Cryptography

- practice and study of hiding information, converting a plaintext into a cipher

Cryptanalysis

- practice and study of penetration or breaking of cryptographic systems, exposing information hidden by cryptography.

Cryptology

- cryptography and cryptanalysis

TRADITIONAL AND MODERN CRYPTOGRAPHY

- **In its traditional definition cryptography is the science of secret writing.**
- **Modern cryptography is very much a mathematical discipline.**

TRADITIONAL AND MODERN CRYPTOGRAPHY

Traditional: Secure communication

- Data confidentiality
- Data integrity
- Data origin authentication

Modern: Solve disputes

- In addition: non-repudiation

CIA AND CRYPTOGRAPHY

- **Data Confidentiality:** **encryption algorithms hide the content of messages.**
- **Data Integrity:** **integrity check functions provide the means to detect whether a message has been changed.**
- **Data origin authentication:** **message authentication codes or digital signature algorithms provide the means to verify the source and integrity of a message.**

CRYPTOGRAPHIC MECHANISMS

Hash functions (integrity check functions, MDCs, MAC)

Digital Signatures

Encryption/decryption

- Symmetric, Private-key
- Asymmetric, Public-key

COMPUTABILITY

- ***Easy to compute*: *computable in polynomial time*.**
- ***Infeasible*: *not computable in polynomial* .**

ONE-WAY TRAPDOOR FUNCTIONS

A one-way function f is a $(1\text{-}1)$ function f s.t.

$y = f(x)$ is easy to compute, but $x = f^{-1}(y)$ is infeasible

A trapdoor function f is a function s.t.

$x = f_k^{-1}(y)$ is easy iff the key k is known

ONE-WAY TRAPDOOR FUNCTIONS

Examples:

- Mixing colors

PROBLEMS OFTEN USED IN CRYPTO

Problems often used in crypto

1 • Discrete Logarithm Problem, DLP:
  Given p, a and $y = a^x \bmod p$, find x

2 • n^{th} root problem:
  Given m, n and a, find b such that $a = b^n \bmod m$

3 • Factorisation:
  Given n, find prime factors

HASH FUNCTIONS

Maps arbitrary-length *m to fix-length hash value h(m)*

- A ”fingerprint” of *m, message digest, ”checksum”*

Desired properties

1. Ease of computation
2. Compression
3. Pre-image resistance: given x, *computationally infeasible to find* m *s.t.* $x=h(m)$
4. Weak collision resistance: given x *and* $h(x)$, *infeasible to find* $y \neq x$ *s.t.* $h(x)=h(y)$
5. Strong collision resistance: infeasible to find pair (x,y) *s.t.* $h(x)=h(y)$

HASH USAGE

1. $m+H(m)$ - no confidentiality or authentication
2. $E_k(m+H(m))$ - auth&conf
3. $m+E_k(H(m))$ - same as MAC
4. $m+E_{eA}(H(m))$ - authentication (digital signature)
5. $E_k(m+E_{eA}(H(m)))$ - and confidentiality
6. $m+H(m+k)$ - authentication without encryption
7. $E_k(m+H(m+k))$ - and confidentiality

MESSAGE AUTHENTICATION CODES

Keyed hash function that provides data origin authentication (verify integrity and source)

Properties:

1 • Ease of computation

2 • Compression

3 • Computation resistance: For secret key k, given a set of pairs $(m_i, C_k(m_i))$ infeasible to compute $C_k(m)$ for a new m

MESSAGE AUTHENTICATION CODE ATTACKS

Brute force attack to find k is no less difficult than finding a decryption key of same length

DIGITAL SIGNATURES

A digital signature scheme consist of 1 **a key generation algorithm,** 2 **a signature algorithm and** 3 **a verification algorithm.**

Digital signatures support non repudiation.

Examples of digital signatures:

- El Gamal
- One time signature
- RSA(Rivest, Shamir, & Adleman)

DIGITAL SIGNATURES

MAC is not enough

- Recipient can fake it since he knows k
- Sender can therefore deny messages

Digital signatures must be

- *unforgeable: impossible for anyone else to make A's signature*
- *authentic: B can check that a message mis-signed by A, and the signature is "firmly attached" to m.*
- *Verify the author, time and date. Authenticates the contents . Verifiable by third party.*

DIGITAL SIGNATURES

Two parts: signature algorithm, verification algorithm.

- Signature uses *private key known only to signer (plus (hash of) data to sign)*
- Verification uses *public key(and signed data)*

DIGITAL SIGNATURES, EXAMPLES

El Gamal, DSA:

- security related to DLP (discrete logarithm problem)

RSA signatures (Rivest, Shamir, & Adleman)

- security related to factorisation
- s =*EkA-(h(m)): encrypt hash value using sender's private key*
- verify: *h(m)=DkA(s): decrypt signature with sender's public key, compare with hash value*

MESSAGE AUTHENTICATION AND DIGITAL SIGNATURE

Message authentication ensures two things: confirming the sender's legitimate and validating that the message hasn't been altered.

Digital signatures go further by providing non-repudiation: ensuring the sender can't deny sending the message.

This process involves two tiers:

- Authentication function
- Authentication protocol (employing the authentication function).

ENCRYPTION

We use "encryption" specifically for algorithms designed to safeguard data confidentiality.

While some encryption algorithms offer methods to detect breaches in integrity, this isn't a universal feature.

Encryption algorithms consistently fall into two categories:

- Symmetric algorithms
- Asymmetric algorithms

AUTHENTICATION BY ENCRYPTION

Public-key encryption

- *$c = E_{dB}(m)$ gives confidentiality but no authentication*
- *$c = E_{eA}(m)$ gives authentication but no confidentiality*
- *$c = E_{dB}(E_{eA}(m))$ gives both*
- B cannot forge messages, and A cannot deny them
- Still needs checksum for arbitrary data

ENCRYPTION ALGORITHMS

Encryption algorithms can be categorized into block ciphers and stream ciphers based on two distinguishing criteria:

- Block size
- Key stream

BLOCK SIZE

- **The block cipher encrypts sizable data blocks, often around 64 bits, employing a complex encryption function.**
- **It encrypts all blocks from the same document using a single key.**
- **The security of a block cipher relies on the intricacies and robustness of its encryption function design.**

KEY STREAM

- A stream cipher encrypts smaller units of data, usually bits or bytes, using a straightforward encryption function.
- It encrypts data under a dynamically changing key stream.
- The security of stream ciphers hinges on the design of the key stream generator.

SYMMETRIC ALGORITHMS

- A single key is utilized for encryption and decryption purposes and must be kept confidential.
- All parties possessing this shared key can decrypt and access data encrypted under that specific key.

ASYMMETRIC ENCRYPTION ALGORITHMS

Also called public key algorithms,

Different keys are used for encryption and decryption.

The encryption key can be made public,

The decryption key has to remain private.

CRYPTOGRAPHIC STRENGTH

Strength of algorithm and key –not by secret algorithms (security by obscurity)

- *empirically secure*
- *provably secure*
- *unconditionally secure*

EMPIRICALLY SECURE

- An algorithm is empirically secure when it has endured over time without revealing significant weaknesses under prolonged analysis.
- While there's no definitive proof that the algorithm might not succumb to a novel and innovative attack in the future, its acceptance within the cryptographic community signifies trust and recognition.

PROVABLY SECURE

- Provably secure algorithms fulfill the longstanding aspiration of computer security.
- An algorithm is deemed secure if breaking it is at least as challenging as solving another problem known to be arduous.

UNCONDITIONALLY SECURE

- An unconditionally secure algorithm remains impervious to decryption, even when faced with attackers possessing unlimited computing power.
- The concept of unconditionally secure algorithms is rooted in information theory.
- An algorithm is considered secure if an attacker cannot obtain additional information about the plaintext by observing the corresponding ciphertext.

UNCONDITIONALLY SECURE- EXAMPLE

- The classic illustration of an unconditionally secure algorithm is the one-time pad.
- In this method, the sender and receiver share a completely random key stream, utilized only once.
- However, even unconditionally secure ciphers have been compromised when operators reuse the same vital streams more than once.