Systems Security Group | Lancaster University

An Introduction to Cryptography

Learning Objectives

- Learn about cryptosystems
- Understand what cryptosystems offer and where to use

What is cryptography?

- Cryptography is the study of mathematical techniques related to aspects of information security
- A cryptosystem can provide
  - **Confidentiality**: Renders the information unintelligible except by authorised entities
  - **Data integrity**: Ensure that data has not been altered in an unauthorized manner since it was created, transmitted or stored
  - **Authentication**: Can verify the identity of the user or system that created the information
  - **Authorisation**: Upon providing identity information, the individual is then provided with the key or password that will allow access to a resource
  - **Non-repudiation**: Ensure that the sender cannot deny sending the message

Cryptosystem

- A cryptosystem is a five-tuple (*P,C,K,E,D*), where
  - *P*: Finite message space - plain texts
  - *C*: Finite crypto-text space - cipher texts
  - *K*: Finite key space
  - *E*: Encryption function $\mathrm{E_k}: P \rightarrow C, k \in K$
  - D: Decryption function $\mathrm{D_k}: C \rightarrow P, k \in K$
- It holds:

  $$\forall e \in K\ \exists d \in K: \forall m \in P \implies D_d(E_e(m)) = m$$

  e: encryption key

  d: decryption key

https://www.cs.jhu.edu/~scheideler/courses/600.471_S05/lecture_6.pdf

What is a key?

- A key is used as an input to a cryptographic function.
- The security of the cryptosystem is based on the key secret.
  - Kerckhoff's principle: *'A cryptosystem should be secure even if everything about the system, except the key, is public knowledge'*.

One-time pad: Perfect encryption scheme

- XOR's message stream and keystream

Message stream: 1001010111

Keystream: 0011101010

Ciphertext stream: 1010111101

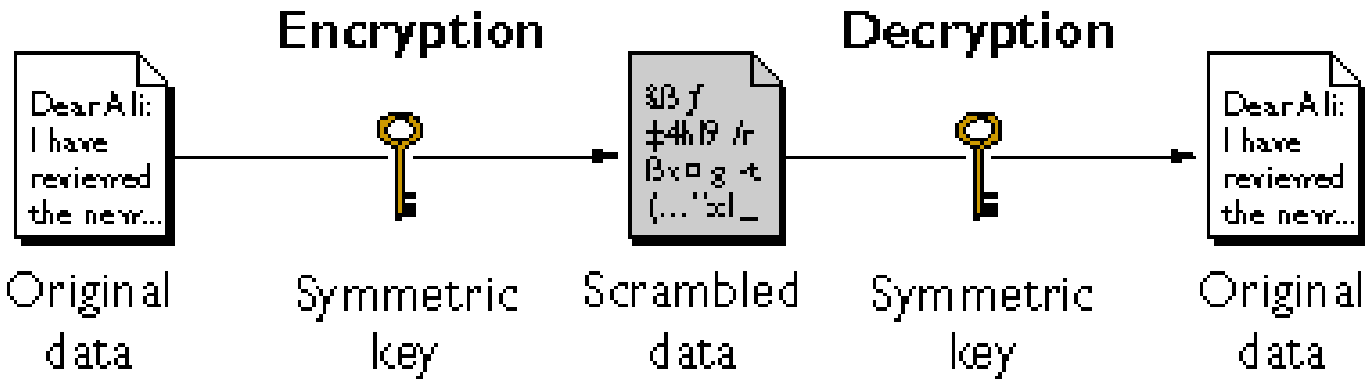
- Deemed unbreakable when:
  - The pad must be used only once
  - The pad must be as long as the message
  - The pad must be securely distributed and protected at its destination
  - The pad must be made up of truly random values

Building blocks of a security system

- Symmetric cryptography
- Asymmetric cryptography
- Message Authentication Codes Vs. Signatures Vs. Hashing

Symmetric cryptography

- A cryptosystem in called symmetric if *d=e* or if *d* can at least be easily computed from *e.*
- Keys required for N parties: N(N-1)/2
- Need for exchanging *e (e.g., Diffie – Hellman)*.



Symmetric cryptography - Types

- Block-based ciphers
  - Encrypt blocks of information at a time
  - Stronger than stream ciphers, but slower.
- Two attributes to look after
  - Confusion (obscurity)
    - Relation of key-ciphertext should be complicated; key can't be determined from ciphertext
  - Diffusion
    - Output should depend in a complex way with the inputs; changing 1-bit should have a significant difference in the output

Symmetric cryptography - Types

- Stream-based ciphers
  - Work with one bit at a time
  - They mix plaintext with key stream
  - Good choice for real-time services
  - They are fast and easy to implement in hardware
  - Key is often combined with an initialization vector (IV)

Algorithms for symmetric cryptography

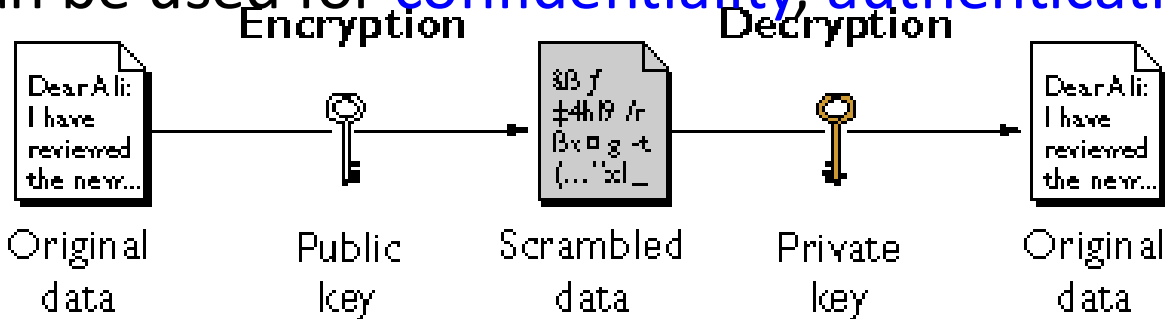
- Data Encryption Standard (DES)
  - DEA is the algorithm
  - DES is the standard
- Triple DES
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA)
- Blowfish
- RC4, RC5

Algorithms for symmetric cryptography

- RC4
  - Stream cipher
  - Use in SSL
  - Improperly implemented in WEP
    - Initialisation vectors: Random values used with algorithms so patterns are not created during encryption
- RC5
  - Block cipher
  - Changeable key size, block size and number of rounds
- RC6
  - Speed improvements over RC5

Asymmetric cryptography

- A cryptographic scheme is called asymmetric if *d* <> *e and* it is computationally infeasible in practice to compute *d* out of *e*.
- In asymmetric cryptography *e* goes public and *d* is kept as a secret.
  - Anybody can use *e* to encrypt a plaintext and only the one that has *d* can decrypt it.
  - Public key cryptographic schemes.
  - Can be used for confidentiality, authentication or both



Algorithms for asymmetric cryptography

- RSA
- Rabin
- El Gamal
- Diffie – Hellman
- Elliptic Curve Cryptography
  - A 256-bit ECC key can be considered equivalent to a 3072-bit RSA key.
  - ECC keys are much smaller than RSA keys.
  - More efficient: computes logarithms of elliptic curves

Advantages and disadvantages

Symmetric

- Strengths
  - High speed encryption
  - Several algorithms use variable key length
- Weaknesses
  - Secure key exchange difficulty
  - Key management difficult

Asymmetric

- Strengths
  - Does not require secure key exchange
  - Provides a method for authentication and digital signatures
- Weaknesses
  - Slow encryption speeds

Cryptographic hash functions

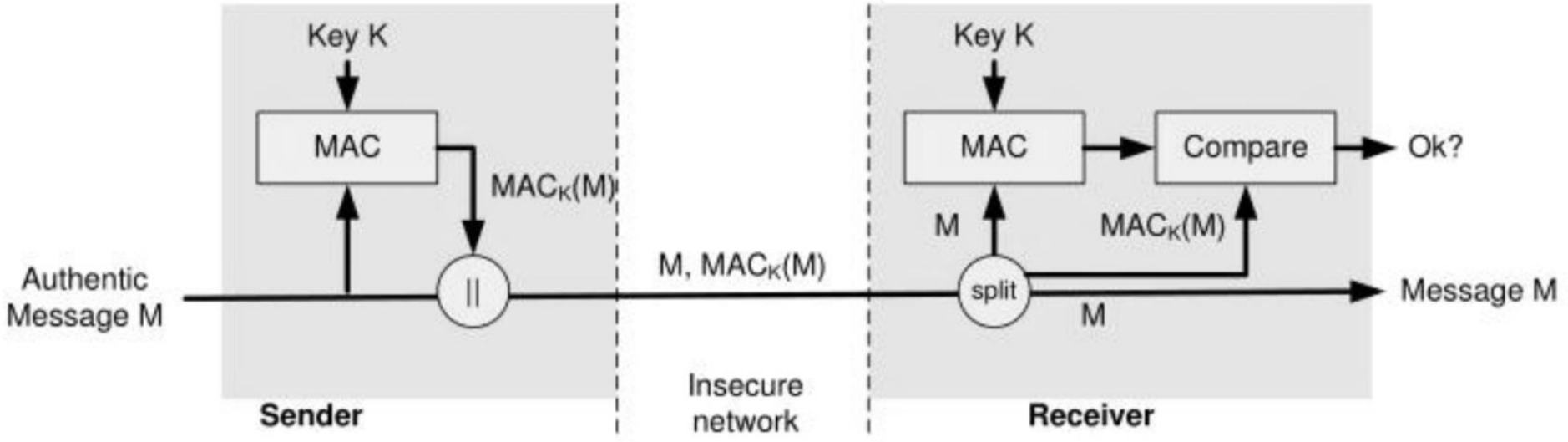
- A cryptographic hash function *H* must provide
  - Compression: e.g, *H*: {0,1}* → {0,1}^{160}
  - Efficiency: H: h(*x*) easy to compute for any *x*
  - One-way: given *y* it is infeasible to find *x*: h(*x*)=*y* (preimage resistance)
  - Weak collision resistance: for any given *x,* it should be difficult to find x' , *x'*≠*x* so that h(*x'*)=h(*x*) (2nd preimage resistance)
  - Strong collision resistance: it should be difficult to find any pair (*x, x'*) with *x*≠*x'* so that h(*x*)=h(*x'*) (collision resistance)

Cryptographic hash functions

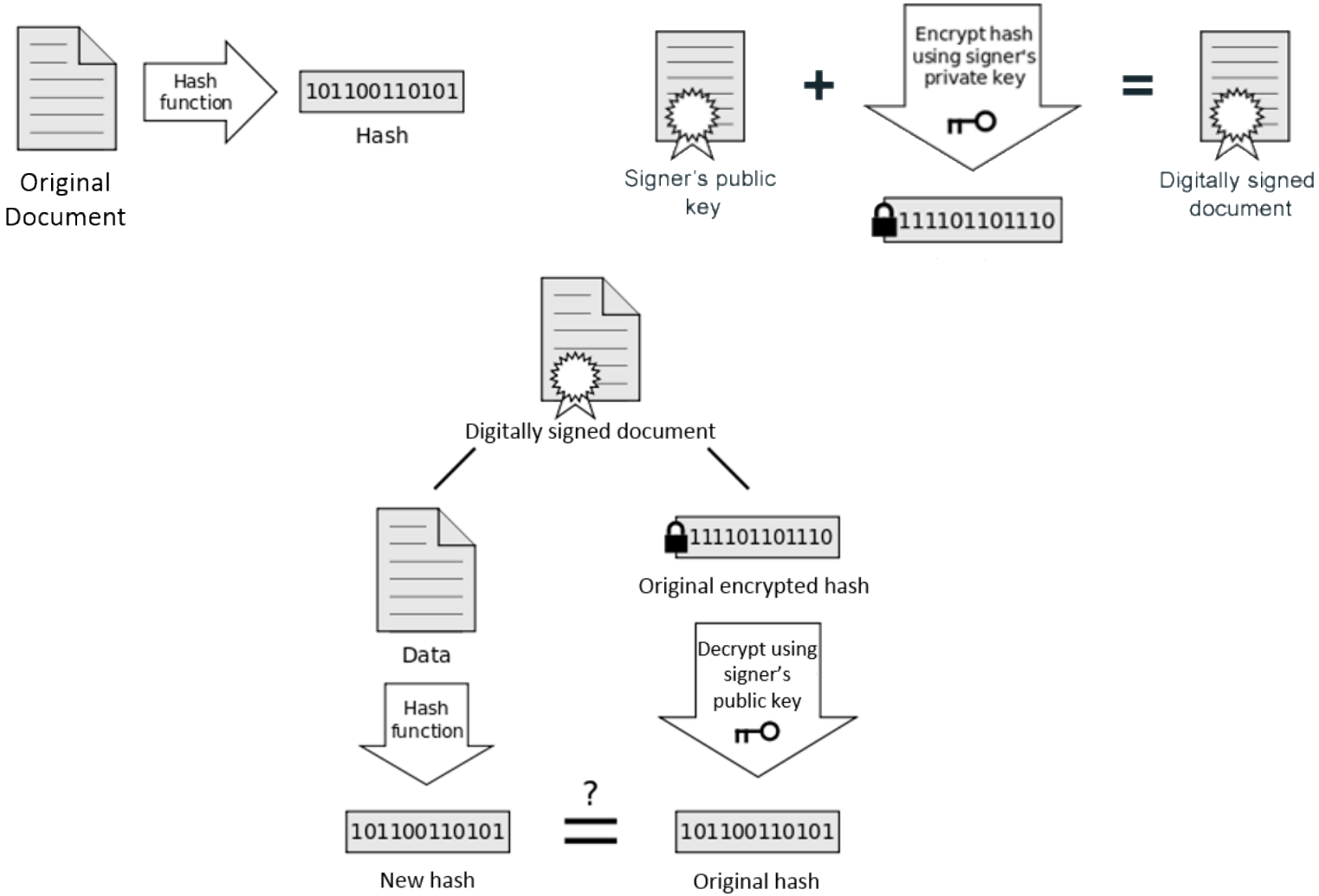
- MD4
  - 128 bit
  - Very fast
  - Has been shown to be broken
- MD5
  - 128 bits
  - Fast
  - Has been shown to have certain weaknesses (collisions can be found easily)
  - Widely used as checksum to verify the integrity of data
- SHA-1
  - 160 bits hash value
  - Standard for US Government
  - Has been shown to have weaknesses
  - Slower than MD5

Message Authentication Codes (MAC)

- MAC prevent tampering with messages
  - Encryption may prevent from reading messages, but doesn't prevent from manipulation



Digital signatures



Hash vs MAC vs Digital signatures

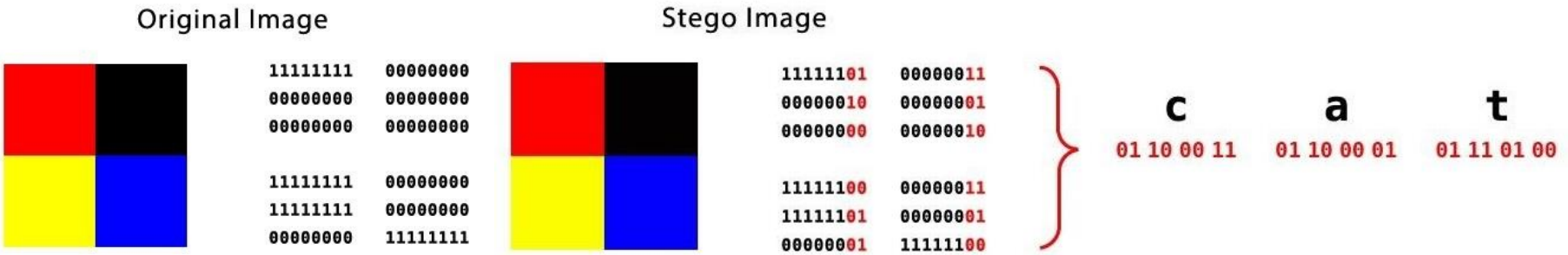
	Hash	MAC	Digital Signature
Authentication	No	Yes	Yes
Integrity	Yes	Yes	Yes
Non-repudiation	No	No	Yes
Key type	N/A	Symmetric	Asymmetric

Security of cryptography

- Integer factorization
  - Result = *p* * *q*, *p*, *q* primes (Prime factorization)
  - Given Result find *p* and *q*
  - 6 = *p* * *q*? (easy) *p*=2, *q*=3
  - How about 49,098,013? And it can get really worse!
- Let a large b-bits number
  - No algorithm that can factor in polynomial time $O(b^k)$
- Not completely true!
  - Shor's algorithm can factor in $O(b^3)$ BUT can be run only on a quantum computer!
- Discrete logarithmic problem: find the unique integer $i \in [0, n-1]: \alpha^i = \beta, i = \log_a \beta,$
  p: prime, α,β nonzero integer mod p
  Find $x: a^x \equiv b \; mod \; p$

Steganography

- Hide data in another media type
- Hidden rather than encrypted
- Sometimes use the least significant bit
  - For example, in colour images use the value for colour intensity, not discernible with human eye



Cryptography in networks

- Protecting data while in transit
- Link encryption
  - Protects confidentiality of information within the communications channel only
  - Not prone to traffic analysis
- Network encryption
  - Transparent to users.
  - Independent of any other encryption process used
  - Data encrypted only while in transit.
- End – to – end encryption
  - Encrypts application layer data only.
  - Network devices doesn’t need to be aware.

Encryption of data in use

- Secure sensitive information while a system is actively processing it
- Homomorphic encryption
  - Allows computations on encrypted data without decrypting it first, e.g., Microsoft SEAL
- Secure enclaves
  - Use hardware-based solutions (e.g., Intel SGX)
  - Confidential computing – Cloud frameworks
  - Provide isolated environments for secure data processing
- Balance of security with the need for real-time data processing

Cryptographic attacks

Cryptographic attacks

Goal is to discover the key

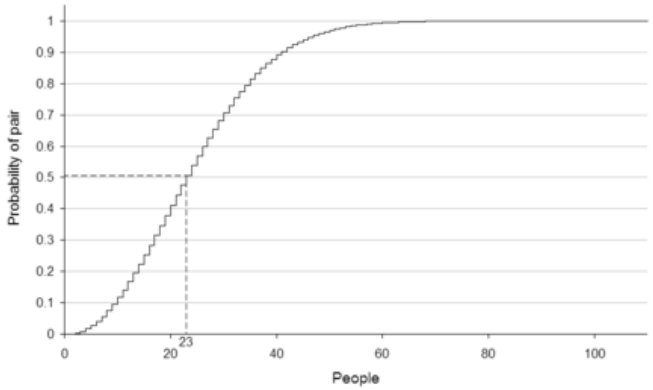
- Cipher-only attack
  - Obtain ciphertext from several messages
  - Encrypted with the same encryption algorithm
- Known-plaintext attack
  - Attacker has plaintext and corresponding ciphertext of one or more messages
- Chosen-plaintext attacks
  - Attacker has the plaintext and ciphertext, but can choose the plain text that gets encrypted
- Chosen-ciphertext attacks
  - Choose ciphertext to be decrypted and study transformation to plain text

Cryptographic attacks

- Differential cryptanalysis
  - Look at statistical differences when encrypting different messages with the same key
- Side-channel attack
  - Gathering ‘outside’ information
  - 1995 RSA private key uncovered by measuring the relative time of crypto operations
- Social engineering attacks
  - Non-technical attacks that are carried out on people

Birthday attack

- Refer to a class of brute-force attacks
- Based on the birthday problem in probability theory
  - The probability that 2 or more people in a group of 23 people to share the same birthday is 50%
  - Raising the group people to 70 increase the probability to 99.9%
- Birthday attacks often used to find collisions of hash functions



Questions?

References

[1] Shon Harris, All in One, CISSP Exam Guide, Chapter on Cryptography
[2] William Stallings, Cryptography and Network Security, Principles and Practise, 5th edition
[3] Birthday attack, https://www.sciencedirect.com/topics/computer-science/birthday-attack