Overview of Cryptography

Prof: Pierre-Alain Fouque

Reference: http://cacr.uwaterloo.ca/hac/about/chap1.pdf

Agenda

- Security objectives and Cryptographic goals
- Cryptographic primitives
- Level of security
- Functions, one-way function and trapdoor one-way function
- Basic definitions
- Symmetric-key cryptography

Cryptography: Security Objectives

- Confidentiality: keeping information secret from all but those who are authorized to see it
- Integrity: ensuring information has not been altered by unauthorized or unknown means
- Entity Authentication: corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.)
- Message Authentication: corroborating the source of information; also known as data origin authentication
- Non-repudiation: preventing the denial of previous commitments or actions
- Anonymity: concealing the identity of an entity involved in some process

Cryptographic Goals

- *Confidentiality :* service used to keep the content of information from all but those authorized to have it. *Secrecy* is a term synonymous with confidentiality and privacy. Numerous approaches to provide confidentiality: physical protection to mathematical algorithms making data unintelligible

- *Data integrity :* service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

- *Authentication :* service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: *entity authentication* and *data origin authentication*. Data origin authentication implicitly provides data integrity (if a message is modified, the source has changed)

- *Non-repudiation :* service which prevents an entity from denying previous, commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.

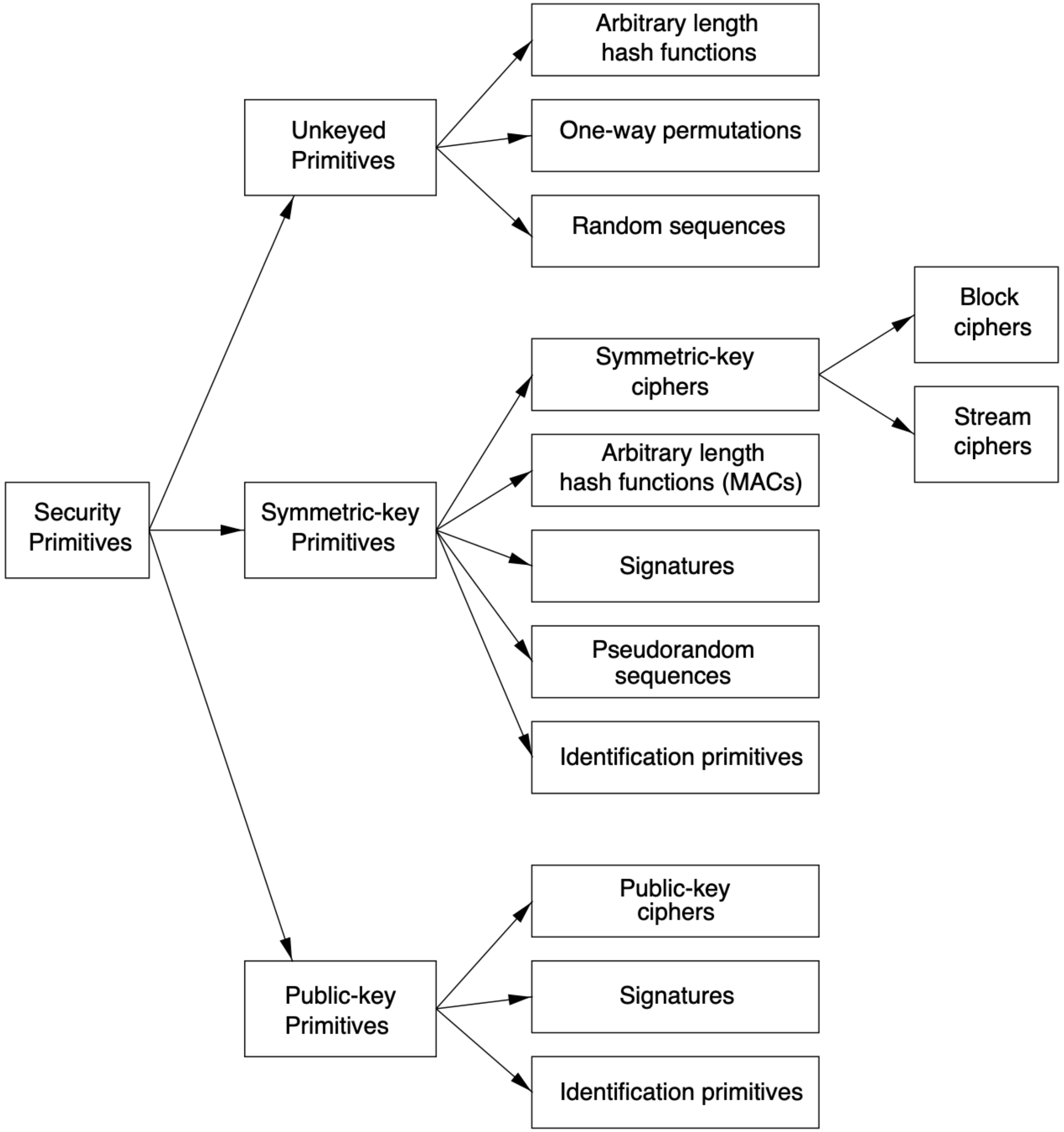
Cryptographic Primitives

Confidentiality: Symmetric-key and public-key ciphers

Integrity: MAC and Signatures

Message Authentication: MAC, Signature

Entity Authentication: Identification primitives



Level of security

- *Level of security: Hard* to quantify. Often, given in terms of the number of operations required (using the best methods currently known) to defeat the intended objective.

Typically the level of security is defined by an upper bound on the amount of work necessary to defeat the objective. This is sometimes called the work factor

- 2^{40} operations: easy to solve using one computer within a day
- 2^{64} operations: middle: possible using many computers or GPU
- 2^{80} operations: hard: probably possible for large agency
- 2^{128} operations: very hard : not possible for anyone

Function (1-1, one-way, trapdoor one-way)

- Function is defined by 2 sets X and Y and a rule f assigning to each element in X precisely one element in Y.
- X is called the domain of the function
- Y is called the codomain or range of the function

- If x is an element of X, written x∈X, the image y of x is the element of Y associated to x; the image y of x is denoted y=f(x)
- Standard notation: f: X→Y
- If y∈Y, then a preimage of y is an element x∈X s.t. f(x)=y
- The set of all elements in Y which have at least one preimage is called the image of f: Im(f)

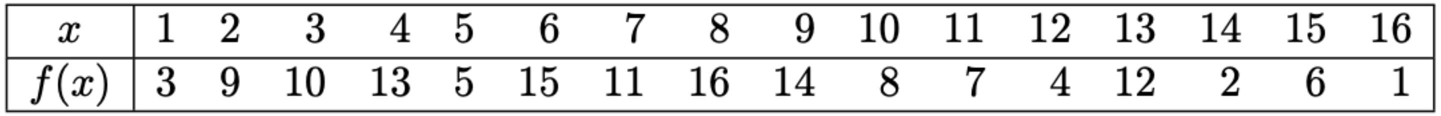
Different kind of functions

- A function is 1-1 (one-to-one) if each element in the codomain Y is the image of at most one element in the domain X
- A function is onto if each element in the codomain Y is the image of at least one element in the domain Im(f)=Y
- A function is called a bijection if it is 1-1 and onto
- If a function is a bijection, we can define its inverse f^{-1} which is the function that for each $y \in Y$, associates its unique preimage
- If S is a finite set. A bijection on S is called a permutation

One-way function

- A function f:X→Y is called a one-way function if f(x) is «easy» to compute for all x∈X but for nearly all elements y∈Im(f), it is computationally infeasible to find x∈X such that y=f(x)

- E.g. X={1,2,3,…,16} f(x)=r_x s.t. the remainder when 3^x is divided by 17



x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

- A prime number is a positive integer greater than 1 whose only positive integer divisors are 1 and itself. E.g. p=48611 and q=53993
- E.g. Factorization: f(p,q) = n (one-way function)

Trapdoor One-way function

- E.g. $n=pq= 2624653723$ and $X = \{1,2,3,\ldots ,n-1\}$
- Define $f(x)=r_x$, the remainder of x^3 divided by n
- For instance, $f(2489991) = 2489991^3 = 5881949859 \cdot n + 1981394214$
- Computing the modular cube root when n is a product of two large prime numbers is a hard problem, while computing the function f is relatively easy (fast modular exponentiation)

- Trapdoor one-way function: f is a one-way function s.t. given a trapdoor, it is easy to invert for any $y \in \mathrm{Im}(f)$
- E.g. RSA cryptosystem

Basic terminology and concepts (I)

- Encryption domains and codomains
  - A: finite set called the alphabet of definition A={0,1}
  - M: set of messages (plaintexts) space: strings of symbols from A.
  - C: ciphertext space. An element from C is called a ciphertext
- Encryption and decryption functions
  - K set, called the key space. An element from K is called a key.
  - Each element $e \in K$, uniquely determines a bijection from M to C, denoted E_e (it must be a bijection to uniquely recover the plaintext), called the encryption function
  - For each $d \in K$, $D_d : C \rightarrow M$, called the decryption function
  - The process of applying E_e to $m \in M$ is called the encryption of m
  - The process of applying D_d to $c \in C$ is called the decryption of c

Basic terminology and concepts (II)

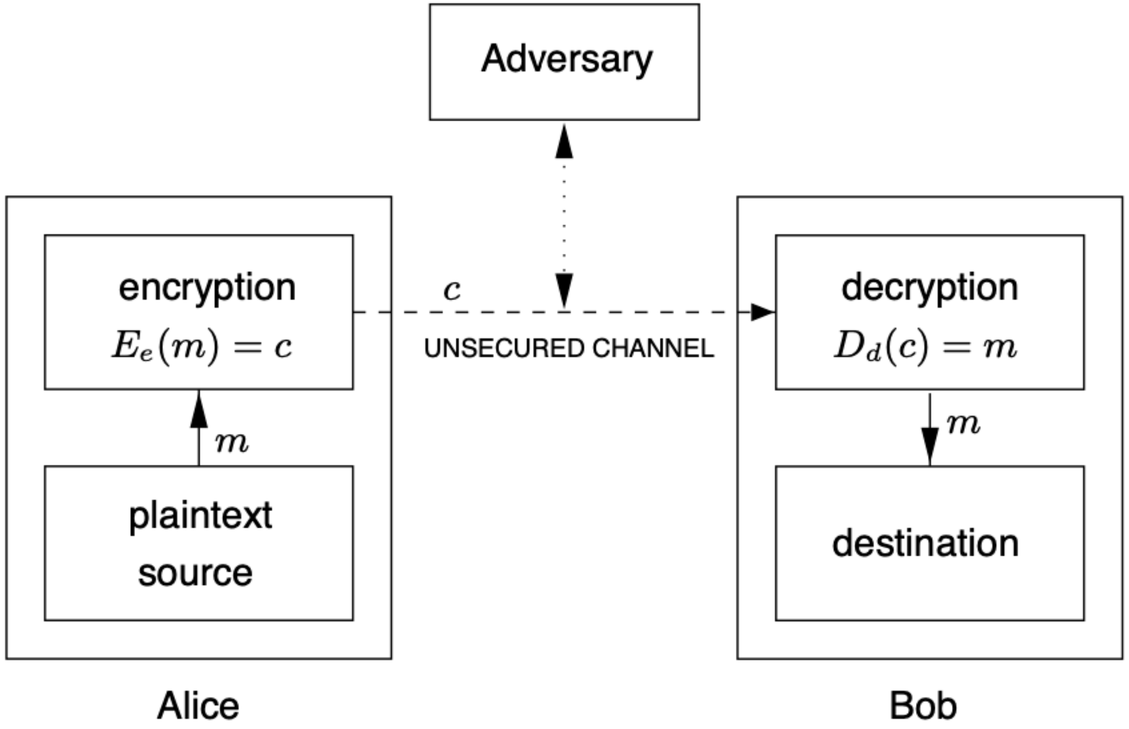
- An encryption scheme consists of a set $\{E_e : e \in K\}$ of encryption functions and a corresponding set $\{D_d : d \in K\}$ of decryption functions s.t. $D_d = E_e^{-1}$, or

  $$\text{for all } m \in M,\ D_d(E_e(m)) = m.$$

  An encryption scheme is sometimes referred to as a cipher.

- The keys e and d are called a key pair and denoted by (e,d). Note that e and d could be the same.
- To construct an encryption scheme requires to select a message space M, a ciphertext space C, a key space K, a set of encryption functions $\{E_e : e \in K\}$ and $\{D_d : d \in K\}$.

Communication Channel



Channel: means of conveying information from one entity to another

Unsecure channel: one from which parties other than those for which the information is intented can reorder, delete, insert, or read.

Secure channel: one from which an adversary does not have the ability to reorder, delete, insert, or read.

Security

- Fundamental premise in cryptography: the sets M, C, and K are public knowledge. When 2 parties communicate securely using an encryption scheme, the only thing they keep secret is the key pair (e,d), they are using and must select

- An encryption scheme is said to be breakable if a third party, without prior knowledge of the key pair (e,d), can systematically recover the plaintext from corresponding ciphertext within some appropriate time frame

- Kerckhoffs' desiderata (1883):
  - System should be, if not theoretically unbreakable, unbreakable in practice
  - Compromise of the system details should not inconvenience the correspondant
  - Key should be rememberable without notes and easily changed
  - Cryptogram should be transmissible by telegraph
  - Then encryption apparatus should be portable and operable by a single person

Cryptography and Adversaries

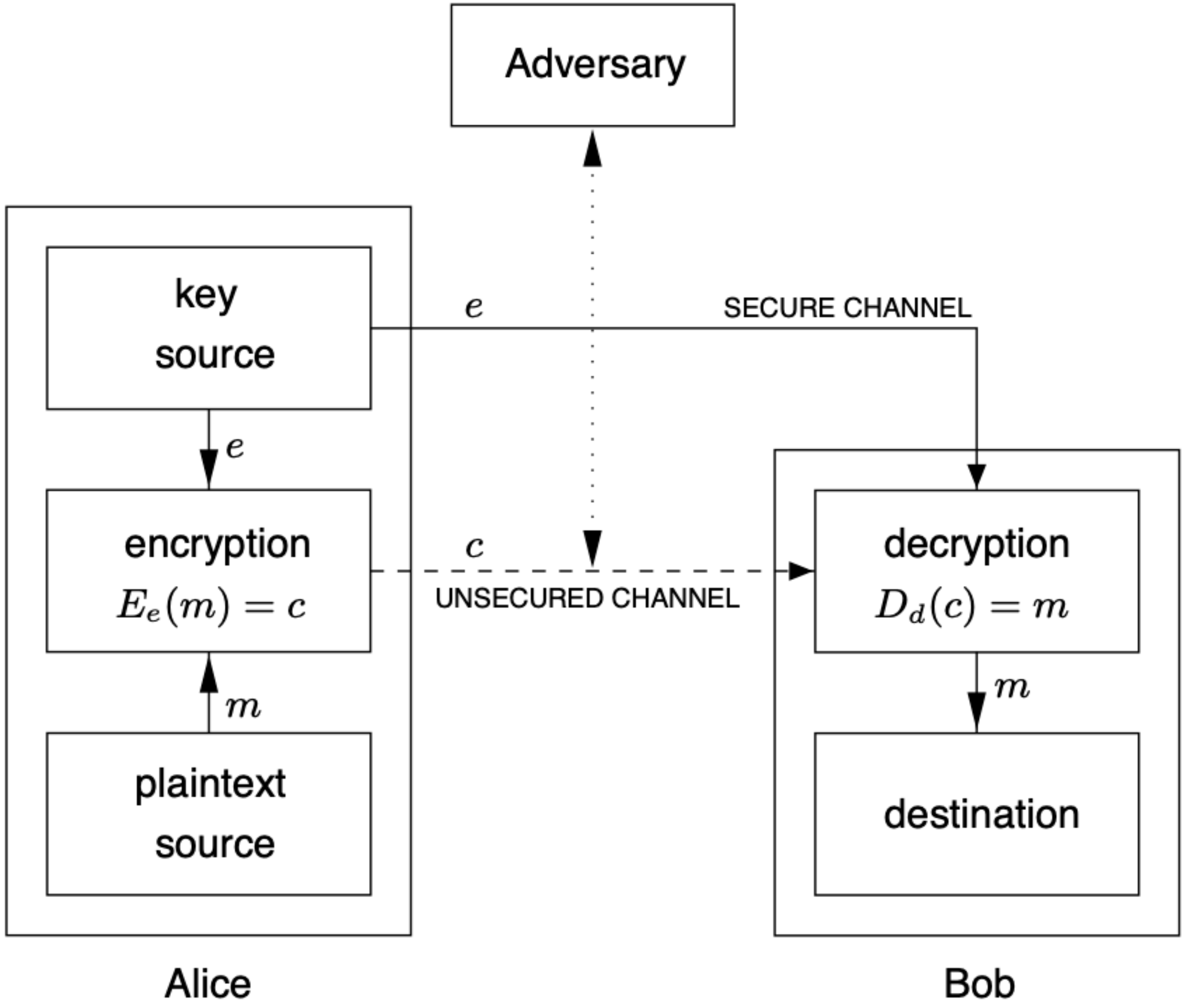
- Passive adversary: an adversary who is capable only of reading information from an unsecure channel
- Active adversary: an adversary who may also transmit, alter, or delete information on an unsecure channel
- Cryptanalysis: the study of mathematical techniques for attempting to defeat cryptographic techniques, or information security services
- Cryptanalyst: someone who engages in cryptanalysis
- Cryptology: study of cryptography and cryptanalysis
- Cryptosystem: general term for a set of cryptographic primitives used to provide information security services

Symmetric-key crypto

Major issue in symmetric-key cryptography, is to find an efficient method to agree upon and exchange keys securely, called as the Key distribution problem

Assumption: the 2 parties know the set of encryption / decryption functions. The only information which must be kept secret is the key d

Two classes of symmetric-key encryption schemes : Block ciphers and stream ciphers



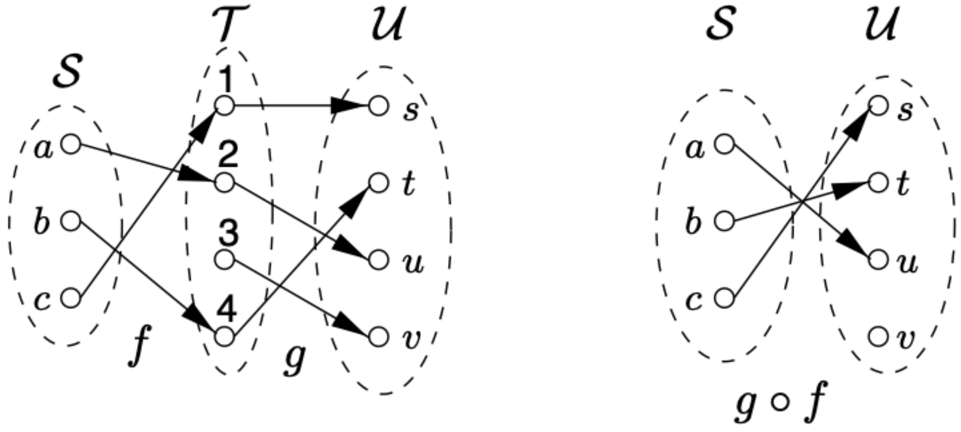
Substitution ciphers

- Substitution ciphers : replace symbols (or group of symbols) by other symbols or groups of symbols.
- Let A be an alphabet of q symbols and M be the set of all strings of length t over A, note A^t. Let K be the set of all permutations on A. For each $e \in K$, $E_e(m) = (e(m_1)e(m_2)\ldots e(m_t)) = (c_1c_2\ldots c_t)=c$ where $m=(m_1m_2\ldots m_t) \in M$.
- Homophonic substitution cipher:
- aa → {0000, 0010, 1000, 1010}   ab → {0001, 0011, 1001, 1011}
- ba → {0100, 0110, 1100, 1110}   bb → {0101, 0111, 1101, 1111}

Transposition ciphers and composition

- Another class of symmetric-key ciphers which simply permutes the symbols in a block

- Let S, T and U be 3 finite sets and let f:S→T and g:T→U.
- The composition gof is the function S→U.



Block-ciphers vs. Stream Ciphers

- A block cipher is an encryption scheme which breaks up the plaintext messages to be transmitted into strings (called blocks) of a fixed length t over an alphabet A, and encrypts one block at a time

- Let K be the key space for a set of encryption transformations. A sequence of symbols $e_1e_2e_3....e_i \in K$, is called a keystream. Let A be an alphabet of q symbols and E_e be a simple substitution cipher with block length 1 where $e \in K$. Let $m_1m_2m_3...$ be a plaintext string and $e_1e_2e_3...$ a keystream from K.
- A stream cipher takes the plaintext string and produces a ciphertext string $c_1c_2c_3...$ where $c_i=E_{ei}(m_i)$. If d_i is the inverse of e_i, $D_{di}(c_i)=m_i$.