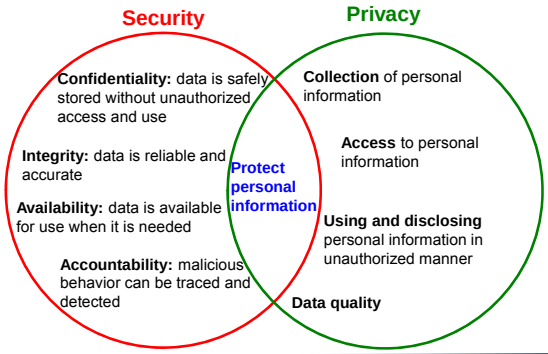
Introduction & Preliminary

What is security and privacy?

What should be considered to ensure security/privacy?

Security vs. Privacy



Security & Privacy in Practice

Security & Privacy Issues

- What to happen?
  unauthorized access, malicious code, data breach…
- Where to happen?
  email communication, internet/networks, could/edge/fog computing, big data, computer/system…
- What result?
  privacy leakage, system collapse, economic loss…

5

- ***What can we do?***
- ***How can we do?***

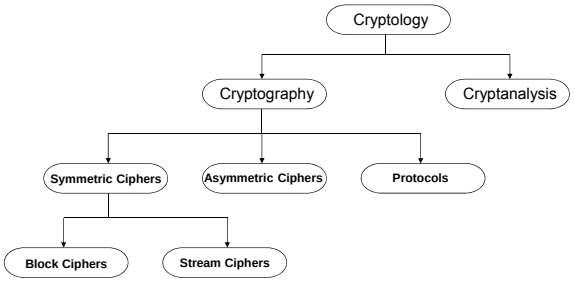
6

What & Why Cryptography?

- "Science of secret writing with the goal of hiding the meaning of a message"
- "Art of writing and solving codes"

7

Overview



8

Security Overview

The Major Goals of Security

- **Confidentiality**
- **Integrity**
- **Availability**
- **Authenticity**
- **Accountability**

Confidentiality

- Confidentiality covers both data confidentiality, and privacy
  - Assure that confidential or private information is not made available or disclosed to unauthorized individuals
- Confidentiality can be preserved by using **encryption**
  - Such as Symmetric Encryption (e.g., DES, AES), and Asymmetric Encryption (e.g., RSA)

Confidentiality: Example

Only Alice and Bob know the contents of the message without learning by others

Confidentiality: Privacy

- Privacy assures that individuals control or influence what information related to them may be collected and stored and by whom, and to whom that information may be disclosed.
- Privacy can be partially preserved via confidentiality
  - Privacy can also be preserved via other means

13

Privacy: Example

The requirements of privacy include:
(1) No one knows the contents of message (confidentiality);
(2) Or no one knows who is the sender/receiver, and so on…

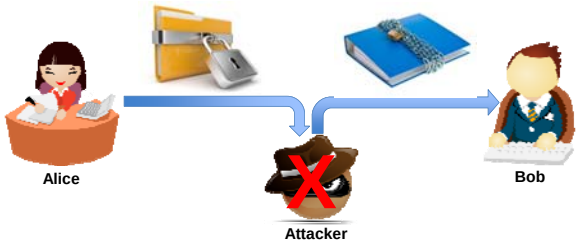
14

Integrity

- Integrity covers both data and system integrity
  - Guarding against improper information modification or destruction
- Data integrity can be achieved by using **message authentication code (MAC)** or **message integrity code (MIC)**
  - MAC and MIC can come from hash functions (such as MD5, SHA) or block ciphers

15

Integrity: Example



No one can modify or destruct Alice's message

16

Availability

- Assures timely and reliable access to and use of information
  - A loss of availability is the disruption of access to or use of information
- Firewall, Intrusion detection system (IDS), load balancer, and antivirus software can be used to achieve availability

17

Availability: Example

Bob can successfully open/read the received message

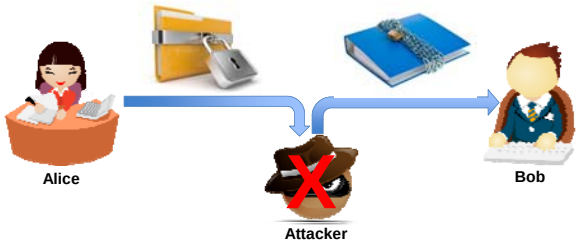
18

Authenticity

- The property of being genuine and being able to be verified and trusted; confidence in the validity of a message, or message originator
  - Authenticity overlaps with integrity
  - Authentication is the process of reliably verifying the identity of someone (or something)
- Authenticiy can be achieved by digital signature (such as DSA)

19

Authenticity: Example



Bob can verify that whether the message is sent from Alice

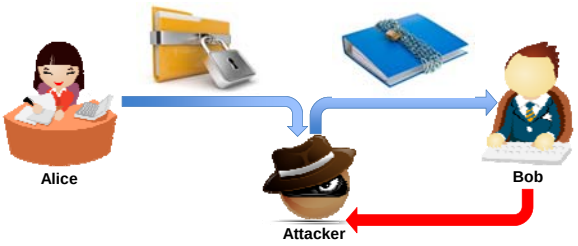
20

Accountability

- The security goal that generates the requirements for actions of an entity to be traced uniquely to that entity
- Various ways to achieve accountability
  - **Logging & auditing**
  - **Digital signature**

21

Accountability: Example



The malicious guys can be identified or traced

22

Basics of Cryptanalysis

23

Why Cryptanalysis?

- There is no *mathematical proof of security* for any practial cipher
- The only way to have assurance that a cipher is secure is to try to break it (and fail) !

Kerckhoff's Principle is paramount in modern cryptography:

A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key.

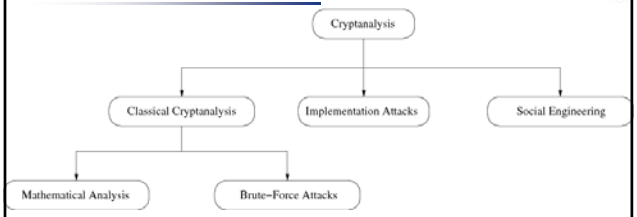
24

Cryptanalysis

- In order to achieve Kerckhoff's Principle in practice: **Only use widely known ciphers that have been cryptanalyzed for several years by good cryptographers!**
- It is tempting to assume that a cipher is more secure if its details are kept secret. However, history has shown time and again that secret ciphers can almost always been broken once they have been reversed engineered.

25

Cryptanalysis: Attacking Cryptosystems



- **Classical Attacks**
  - Mathematical Analysis, e.g., letter frequency attack
  - Brute-Force Attack
- **Implementation Attack**: Try to extract key through reverse engineering or power measurement, e.g., for a banking smart card.
- **Social Engineering**: E.g., trick a user into giving up her password

26

Modular Arithmetic

27

Why Modular Arithmetic?

- Extremely important for asymmetric cryptography (e.g., RSA)
- Some historical ciphers can be elegantly described with modular arithmetic (cf. Caesar later on).

28

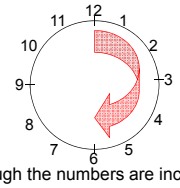
Brief Introduction to Modular Arithmetic (1)

Most cryptosytems are based on **sets of numbers** that are:

1. discrete (sets with integers are particularly useful)

2. finite (i.e., if we only compute with a finiely many numbers)

Let's look at a finite set with discrete numbers we are quite familiar with: a clock.



Interestingly, even though the numbers are incremented every hour we never leave the set of integers:

1, 2, 3, … 11, 12, 1, 2, 3, … 11, 12, 1, 2, 3, …

29

Brief Introduction to Modular Arithmetic (2)

- We develop now an arithmetic system which allows us to **compute** in finite sets of integers like the 12 integers we find on a clock (1,2,3, … ,12).
- It is crucial to have an operation which keeps the numbers within limits, i.e., after addition and multiplication they should never leave the set (i.e., never larger than 12).

Definition: Modulus Operation

Let *a, r, m* be integers and *m* > 0. We write

$a \equiv r \bmod m$

if *(r-a) is divisable by m.*

- "*m*" is called the **modulus**
- "*r*" is called the **remainder**

30

Examples for Modular Reduction

- Let a = 12 and m= 9 : 12 ≡ 3 mod 9
- Let a = 34 and m= 9: 34 ≡ 7 mod 9
- Let a = -7 and m= 9: -7 ≡ 2 mod 9

(you should check whether the condition *m* divides (*r-a*) holds in each of the 3 cases)

31

Properties of Modular Arithmetic (1)

- **The remainder is not unique**

It is somewhat surprising that for every given modulus *m* and number *a*, there are (infinitely) many valid remainders.

Example:

- 12 ≡ 3 mod 9 → 3 is a valid remainder since 9 divides (3-12)
- 12 ≡ 21 mod 9 → 21 is a valid remainder since 9 divides (21-12)
- 12 ≡ -6 mod 9 → -6 is a valid remainder since 9 divides (-6-12)

32

Properties of Modular Arithmetic (2)

- **Which remainder do we choose?**

By convention, we usually agree on the **smallest positive integer *r*** as remainder. This integer can be computed as

quotient remainder

$a = q\ m + r$ where $0 \le r \le m-1$

- Example: $a=12$ and $m=9$

$12 = 1 \times 9 + 3 \quad \rightarrow \quad r = 3$

- **Remark:** This is just a convention. Algorithmically we are free to choose any other valid remainder to compute our crypto functions.

33

Properties of Modular Arithmetic (3)

How do we perform modular division?

- First, note that rather than performing a division, we prefer to multiply by the inverse. Ex:

$$b / a \equiv b \times a^{-1} \bmod m$$

- The inverse a^{-1} of a number a is defined such that:

$$a\ a^{-1} \equiv 1 \bmod m$$

Ex: What is $5 / 7 \bmod 9$?

The inverse of $7 \bmod 9$ is 4 since $7 \times 4 \equiv 28 \equiv 1 \bmod 9$, hence:

$$5 / 7 \equiv 5 \times 4 = 20 \equiv 2 \bmod 9$$

34

Properties of Modular Arithmetic (4)

How is the inverse compute?

- The inverse of a number $a \bmod m$ only exists if and only if:

$$\gcd(a, m) = 1$$

(note that in the example above gcd(5, 9) = 1, so that the inverse of 5 exists modulo 9)

- For now, the best way of computing the inverse is to use exhaustive search.

35

Properties of Modular Arithmetic (5)

Modular reduction can be performed at any point during a calculation

Let's look first at an example. We want to compute $3^8 \bmod 7$ (note that exponentiation is extremely important in public-key cryptography).

- **1. Approach: Exponentiation followed by modular reduction**

$$3^8 = 6561 \equiv \mathbf{2} \bmod 7$$

Note that we have the intermediate result 6561 even though we know that the final result can't be larger than 6.

36

Properties of Modular Arithmetic (6)

- **2. Approach: Exponentiation with intermediate modular reduction**

$$3^8 = 3^4 3^4 = 81 \times 81$$

At this point we reduce the intermediate results 81 modulo 7:

$$3^8 = 81 \times 81 \equiv 4 \times 4 \bmod 7$$

$$4 \times 4 = 16 \equiv \mathbf{2} \bmod 7$$

Remark: If $a1 \equiv r1 \bmod m$ and $a2 \equiv r2 \bmod m$, we have $a1 \times a2 \bmod m = r1 \times r2 \bmod m$

General rule: For most algorithms it is advantageous to reduce intermediate results as soon as possible.

37

An Algebraic View on Modulo Arithmetic: The Ring Z_m (1)

We can view modular arithmetic in terms of sets and operations in the set. By doing arithmetic modulo m we obtain **the integer ring Z_m={0,1,2,…,m-1}** .with the following properties:

- **Closure**: We can add and multiply any two numbers and the result is always in the ring.
- Addition and multiplication are **associative**, i.e., for all a,b,c in Z_m
  - $a + (b + c) = (a + b) + c$
  - $a \times (b \times c) = (a \times b) \times c$

  and addition is **commutative**: $a + b = b + a$
- The **distributive law** holds: $a \times (b+c) = (a \times b) + (a \times c)$ for all a,b,c in Z_m

38

An Algebraic View on Modulo Arithmetic: The Ring Z_m (2)

- There is the **neutral element *0* with respect to addition**, i.e., for all a in Z_m
  - $a + 0 \equiv a \bmod m$
- For all a in Z_m, there is always an **additive inverse element *–a*** such that
  - $a + (-a) \equiv 0 \bmod m$
- There is the **neutral element 1 with respect to multiplication**, i.e., for all a in Z_m
  - $a \times 1 \equiv a \bmod m$
- The **multiplicative inverse a^{-1}**
  - $a \times a^{-1} \equiv 1 \bmod m$

  exists only for some, but not for all, elements in Z_m.

39

An Algebraic View on Modulo Arithmetic: The Ring Z_m (3)

- We recall from above that an element a in Z_m has a multiplicative inverse only if:

$$\gcd(a, m) = 1$$

- We say that a is **coprime** or **relatively prime** to m.

Ex: We consider the ring Z_9 = {0,1,2,3,4,5,6,7,8}
The elements 0, 3, and 6 do not have multiplicative inverses since they are not coprime to 9.
The inverses of the other elements 1, 2, 4, 5, 7, and 8 are:

$1^{-1} \equiv 1 \bmod 9$	$2^{-1} \equiv 5 \bmod 9$	$4^{-1} \equiv 7 \bmod 9$
$5^{-1} \equiv 2 \bmod 9$	$7^{-1} \equiv 4 \bmod 9$	$8^{-1} \equiv 8 \bmod 9$

40

An Algebraic View on Modulo Arithmetic: The Ring Z_m (4)

A ring is a structure in which we can always add, subtract and multiply, but we can only divide by certain elements (namely by those for which a multiplicative inverse exists).

- For all *a, b* in Z_m, we have
  - $a + b \equiv c \bmod m$, where *c* is in Z_m
  - $a \times b \equiv c \bmod m$, where *c* is in Z_m
- Ex: We consider the ring $Z_9 = \{0,1,2,3,4,5,6,7,8\}$

41

- Exercise: Compute the results without a calculator:
  - (-11) x 29 mod 13
  - 3^{16} mod 13

42