Case Study:

Viasat's KA-SAT in Europe was attacked by malware. Company kept a private network open to update remotely. The server was not able to handle that large number of requests.

satellite Network

Friday labs are for collaboration time, lab exercises,

### Definition

Security is relative to

a set of desired properties

an adversary (who conducts malicious activity) with specific capabilities

Ex. Standard file access permissions in linux are not effective against an adversary who can boot from a CD

### Security Goals CIA

#### Confidentiality

Def = avoidance of unauthorized disclosure of information

Ex. disclose sensitive data

Tools:

Encryption = to establish confidential communication over an insecure channel that is subject to eavesdropping

* converting human-readable text into incomprehensible text:

plaintext M=D(C) —encrypt E —> ciphertext C=E(M)

* Caesar Cipher (shift all letters by certain number
* Symmetric key distribution n\*(n-1)/2 keys

A send C = E(M) with key K

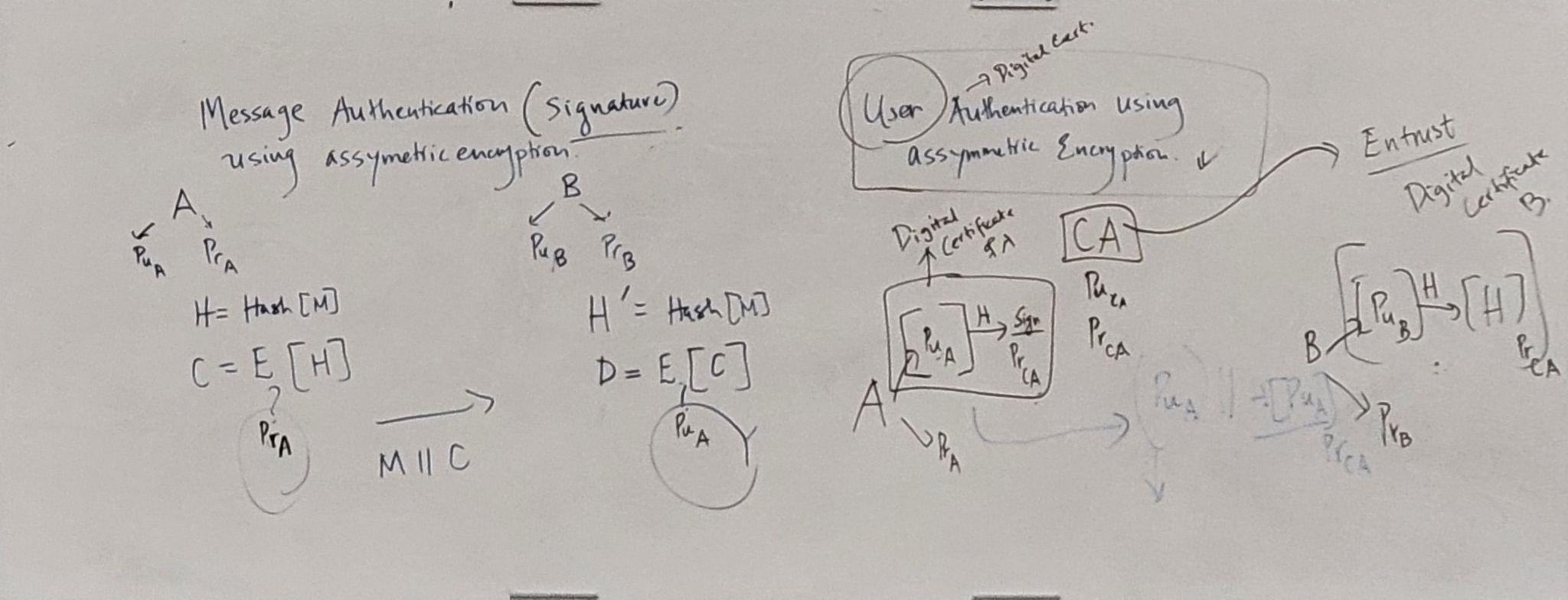
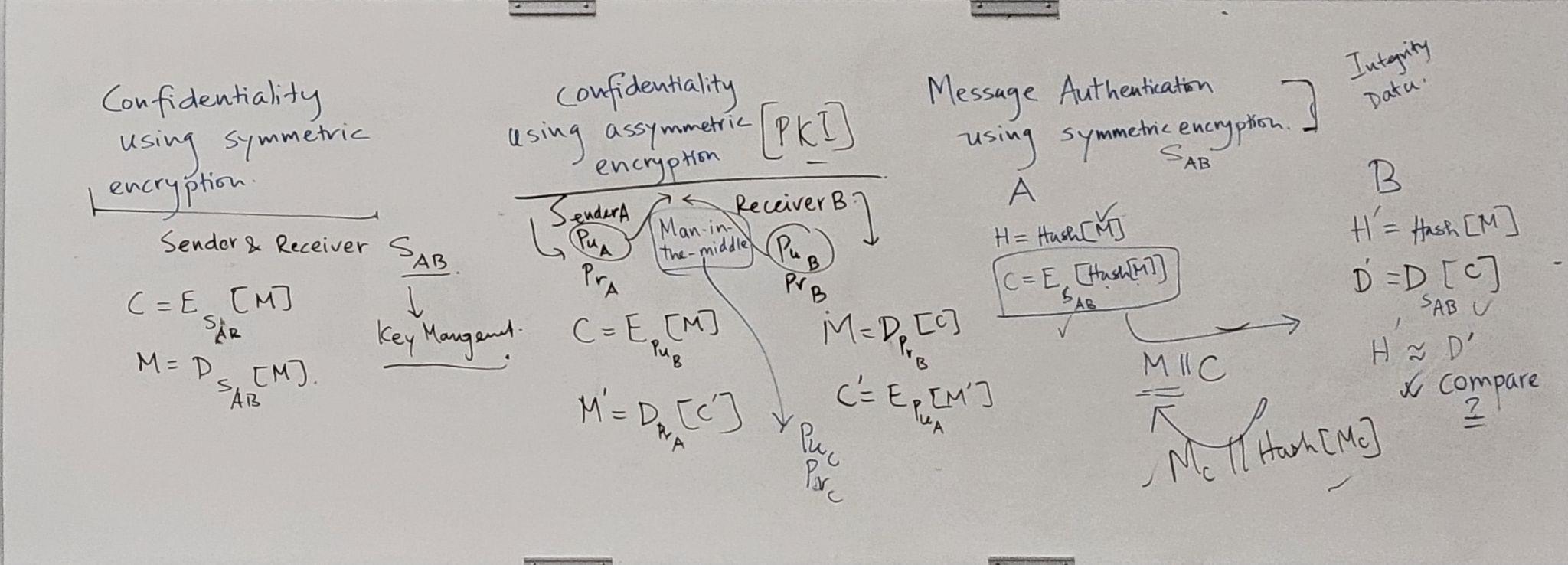
B decrypt M = D(C) with key K

* Asymmetric encryption (PKI): public key only needs 1 key for each recipient

A send C = E(M) with B’s public key

Only B’s private key can decrypt M=D(C)

Problem: C can tell A a different B’s public key, and miscommunication occurs

* Message Authentication Code is for message integrity

Access Control = rules + policies that limit access to confidential data

* least privilege
* role-based access control

Authentication = determination of the identity and role (has knows is)

* Hash functions

Compare H’ and morph D

* Digital Signature/Certificates: message authentication with asymmetric encryption

A sign with A’s private key

Only decrypt correctly with A’s public key

* User authentication using asymmetric encryption

Digital Certificate A:

CA (Entrust) has the

Verification

* Password

Complexity + length + password salt (hash(password))

B = number of bits of the random salt and D=size of list of words

* Magnetic Stripe Cards

Smart card provide secure authentication mechanism and increase the difficult to duplicate the card

SIM card vulnerability cause multi-factor authentication vulnerability

RFIDs = Radio frequency IDs (passports)

* Biometric uniquely identify a person based on biological traits

Features: university, distinctiveness, permanence, collectability (be able to collect, store, and verify)

Fingerprints, retinal, DNA… needs big data to train models

* Social Engineering

pretexting: create a story that convinces administrator into revealing secret information

baiting: gift to get a user/agent to perform an insecure action

quid pro quo: offering an action/service and then expecting something in return

Authorization = determination if a person is allowed to access

Physical Security = establishment of physical barriers to limit access to protected computational resources (Faraday cages)

#### Integrity

Def = data is authentic, accurate, and reliable (not altered in an unauthorized way)

Tools:

Backups = periodic archiving of data

Checksums = assigned value for the purpose of detecting errors that may have been introduced during its transmission or storage

#### Availability

Def = information is accessible and modifiable by authorized users

ex. making website unusable)

Tools:

Physical protection = infrastructure meant to keep information available in physical challenges

Computational redundancies =

### Other Security Concepts AAA

Assurance = how trust is provided/managed in computer systems

Tools (Trusted management depends on):

Policies = behavioral expectations

Permissions = allowed behaviors to interact with a person/system

Protections = mechanisms to enforce permissions and policies

Authenticity = determining that statements, policies, and permissions issued by person/system are genuine

digital signature is the primary tool ( in Confidentiality > Tools > Encryption)

Nonrepudiation = authentic statement that someone/system cannot deny

Anonymity = records/transactions not tied to any individuals

Tools:

Aggregation = combining data in a group so individual data is not trackable

Mixing = intertwining of transactions/information/communications in a untraceable way to an individual

Proxies = tested agents who are willing to engage in actions for an individual in a way that cannot be traced back to that person

Pseudonyms

### Threads and Attacks

Eavesdropping =

Alteration = unauthorized modification of infor (Ex. main-in-the-middle attack = network stream is intercepted)

Denial-of-service (Ex. email spam)

Masquerading = fabrication of information that is purported to be form someone else

Repudiation = denial of a commitment or data receipt

Correlation and traceback = integration of multiple data sources to determine the source of a particular data

### Ten Security Principles

Economy of mechanism

simplicity in design and implementation of security measures

Fail-safe default

default configuration should be conservative protection scheme

Complete mediation

every access must be checked for compliance with a protection scheme (lock time after certain failures)

Open design

security architecture and design should be made publicly available

Separation of privilege

multiple conditions required to get access to restricted resource

Least privilege

program/user should operate with the minimum privileges necessary

Least common mechanism

minimize sharing among one/more users

Psychological acceptability

well designed and intuitive

Work factor

trade off between cost and security

Compromise recording

more desired to record an intrusion

#### Direct Attacks on Computational Devices

Environmental Attacks

Electricity, temperature, limited conductance.

if the warning sensor is disabled by the environmental effects

Eavesdropping = interception of data (secretly listening to private conversation (shoulder phishing?) )

protection…

Wiretapping: put a device between a computer and a cable and receive the information transferring between them.

Acoustic Emissions = translate the sound of user’s typing to get what they are typing

Hardware Keylogger = USB keyloggers installed between keyboard and computer

Tools against direct attack:

TEMPEST = standards for limiting information-carrying electromagnetic emanations

Emanation Blockage = sensitive equipment to block acoustic emanations…

Triple DES cryptosystem on ATMs (be aware of possible attacks)

atm attacks: lebanese loop, skimmer, fake atms

#### Operating Systems and File System Security

Components: I/O — CPU — RAM — Disk

Boot Sequence

Booting/Bootstrapping = loading an OS into memory from a power-off state

BOIS (basic input/output system) is where computer first executes code when turned on

BOIS password …

Hibernation = store states in hibernation file before power-off

Secure vs. Verified Boot (ensure integrity)

minimize attack surface

Disk Encryption

SRK in TPM(trusted encryption module) encrypts VEK (volume encryption key)

SRK uses symmetric encryption key

SRK to store keys outside of the disk

VEK (volume encryption key) in volume metadata encrypts FVEK (internal key)

Why VEK?

if the VEK is taken out, problem with updating the FVEK or scenario. Without VMK, we need to update FVEK and CleartextData, which can be big size, and we also need to update TPM. The advantages of having VEK is that we don’t need to deal with massive updating when updating FVEK

FVEK (full volume encryption key) in volume metadata encrypts the data.

File System Encryption

Encryption

File is encrypted by FEK(File Encryption Key)

FEK is encrypted with users public key (hackers needs user’s private key to decrypt)

Decryption

Encrypted File is decrypted by user’s private key to FEK

File is decrypted by FEK

Processes

RAM is address space

OS controls RAM processes (if hacker get access to RAM, they have access to OS process at some level)

Buffer Overflow: user input exceeds the max length of a valid input => RAM is overwritten unintendedly (can be an attack)

Program Memory Stack and Function Call Stack

Buffer Overflow: Heart Bleed Attack as

The server is not checking if len(message in the request) = length of message in the request => overread

Overread will disclose some sensitive data like customer’s private key

If private key is stolen, all documents signed with the public key must be re-signed with the new key

Command Injection

execute commands via a vulnerable application.

eg. printing !”; rm -rf /\*; echo “! => echo “!”; rm -rf /\*; echo “!”

For each user input, perform length check, format check

Integer Overflow

Ariane 5 rocket to wrong direction,

Always test the system thoroughly if there is any changes in this area

File Access Race Condition [ex](https://www.bugsnag.com/blog/bug-day-race-condition-therac-25):

Processing data in parallel

an attacker can alter the file between the two accesses / operations and replace the file completely.

VM = OS running software???

Dropbox Case Study

Every session should be authenticated

After the first authentication, dropbox put a string and use it to update authentication

Dangerous If a session never expires without repeatedly authentication

[Uber Security News](https://www.nytimes.com/2022/10/05/technology/uber-security-chief-joe-sullivan-verdict.html)

### Malicious Software

#### Malware

Propagation:

virus = human-assisted propagation

worm = automatic propagation

Concealment

rootkit = modifies OS to hide its existence

trojan provides desirable functionality but hides malicious operation

Insider attack = security hole created in a system by one of its programmers

Backdoors = hidden feature/command that allows a user to perform undesired actions

usually used by developer to debug for clients, but increase security vulnerability

Logic Bombs

don’t use someone’s code without understanding what it’s doing

code review before going into the system

Ways to prevent

Avoid single points of failure.

Use code walk-throughs.

Use archiving and reporting tools.

Limit authority and permissions.

Physically secure critical systems.

Monitor employee behavior.

Control software installations.

#### Virus

Def = computer code that can replicate itself by modifying other files/programs

its replication is the main distinction between virus and logic bomb

Phases

Dormant phase: exists and lay low to avoid detection

Propagation phase: replicating itself, infecting new files on new systems.

Triggering phase: some logical condition => perform its intended action

Action phase. performs the malicious action, called payload.

– This action could include something seemingly innocent, like displaying a silly picture on a computer’s screen, or something quite malicious, such as deleting all essential files on the hard drive.

Infection Types

overwrite (delete library and replace with itself)

pre-pending (compress original and insert itself to keep the same size)

infection of libraries (some )

macro viruses: infects MS Office documents (reason why they are read-only by default on open)

#### Concealment

Encrypted virus

Decryption engine + encrypted body

Randomly generate encryption key

Detection looks for decryption engine

Polymorphic virus

Encrypted virus with random variations of the decryption engine (e.g., padding code)

Detection using CPU emulator

Metamorphic virus

different virus bodies for different infection + different decryption engine

Approaches include code permutation and instruction replacement

Challenging to detect

#### Worms

Def = propagate by finding and infecting vulnerable hosts

Trojan horse = software seems to perform correctly but actually perform malicious tasks

Rootkits modifies OS and anti-virus software will not find it because it has more privileges

hard to detect

#### Other Information

honeynet = decoy network that contains one or more honeypots

is used to detect attacks, collect attack data, and study the behavior of attackers

to learn the malware, we can look at the table of functions, the libraries it’s using (critical functions can found in [this article](https://canvas.eee.uci.edu/courses/49765/modules/items/1956392))

### Network Components

#### Def

LAN = Local Area Network for small groups of systems (10-100)

WAN = Wide Area Network (100-1000)

Internet

WAP = Wireless Access Point

ISP = Internet service provider

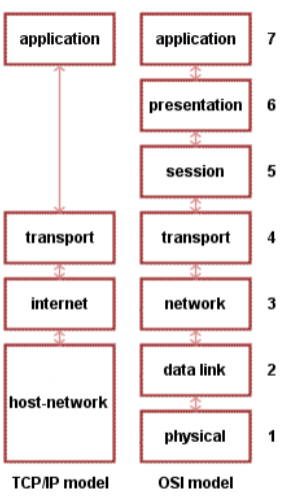
#### Network components

NIC = network interface card allows wires/wireless digital communication

Switch connects multiple network devices inside a LAN

Router routes network traffic between LANs and WANs

|  | Wireless | Wired |
| --- | --- | --- |
| Pros | Cheaper and easier to install  • Generally cheaper to maintain  • Extremely flexible! Devices can leave  and join network throughout the day | • Higher bandwidth (faster upload/download speeds)  • Not subject to interference by other wireless  devices (phones, radios, etc.) |
| Cons | Lower bandwidth (slower network  speed)  • Subject to interference by wireless  devices, as well as microwaves and  other appliances | • Cost of installation is high due to routing of cables  and (potentially) additional network devices  • Less flexible  • Generally, costlier to maintain and troubleshoot  problems |

Layered models

for interconnecting network protocols => for end-to-end network communication

protocol independence and modularity

OSIs (Open Systems Interconnection) model

TCP/IP Model

Data Encapsulation

Process

Sender: top down

User enter a url => find the table for url and ip address in the host => not found, find it in the DNS

send the request to the ip address

if the request is a web server => get the port

for web server, port in transport (multiple programs running in different ports)

In DL, send mac, ip, mac, data to switch

switch finds which browser/port by its ip address

listen to the port

Receiver: bottom up

decrypt => check if it is ip address and port match => send the response in the port to the switch

Sender:

check if ip address and port match => APP get the website information

Because there are so many steps, there are more vulnerabilities

Network Protocols

define rules of communication between network devices

define specific formats for messages exchanged between systems

support message acknowledgement, data compression, and other mechanisms for efficient and reliable communication

sync data after sending it out

Physical Layer

for transmission of bits

consideration: speed? secure? meet bandwidth requirements? practical to install?

Data Link Layer

Stores frame headers (one of the most important part)

MAC address = media access control (layer 2)

identifies a device to other devices on the same local network

access point is based on mac address

pin a computer from the same local network will use mac address

based on switching

Switching is to switch data packets between devices on the same network (or same LAN - Local Area Network)

cannot be changed (hardcoded into device)

IP address = internet protocol

identifies the device globally (layer 3)

4\*8 = 32 bit

controls how devices communicate globally

based on routering

Routing is to Route packets between different networks (between different LANs - Local Area Networks).

can be changed (assigned by software config)

Network layer

delivers data between hosts (different networks)

use packet as protocol data unit

default gateway

used to pass information when the device doesn't know where the destination is

it’s the exit point for all the packets in your network that have destinations outside your network

try to match the prefix with the ip address in the local network. If matches, use ARP (Address Resolution Protocol) to resolve the mac address to an ip address. If not found, it’s trying to go outside. Use ICMP (Internet Control Message Protocol) to allow hosts to communicate network conditions

DHPC

nslookup looks up dns for ip address?

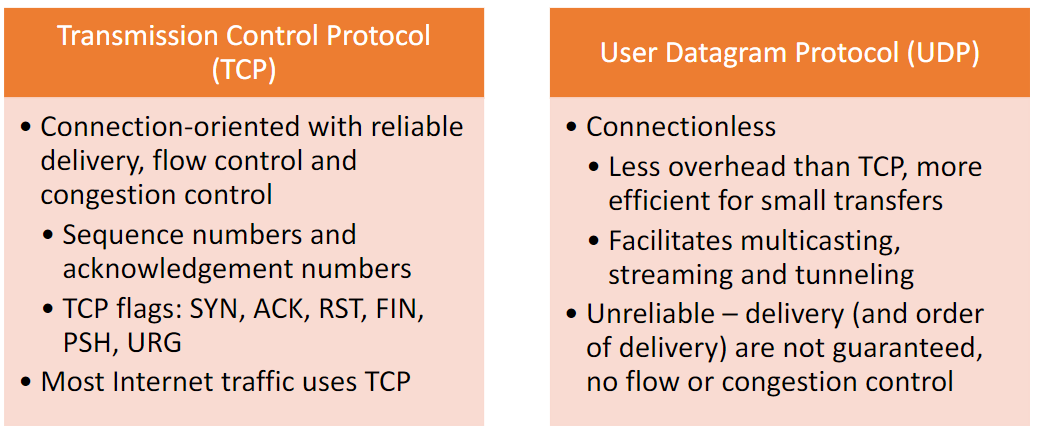
Transport Layer

deliver data from a process on one host to a process on another host (1 ip address can have many ports running multiple processes?)

port number used to get data to the correct process on a host

TCP (transport layer protocols) and DCP

TCP tracks sequence number to reconstruct multiple packets (check if there are more or fewer packets received)



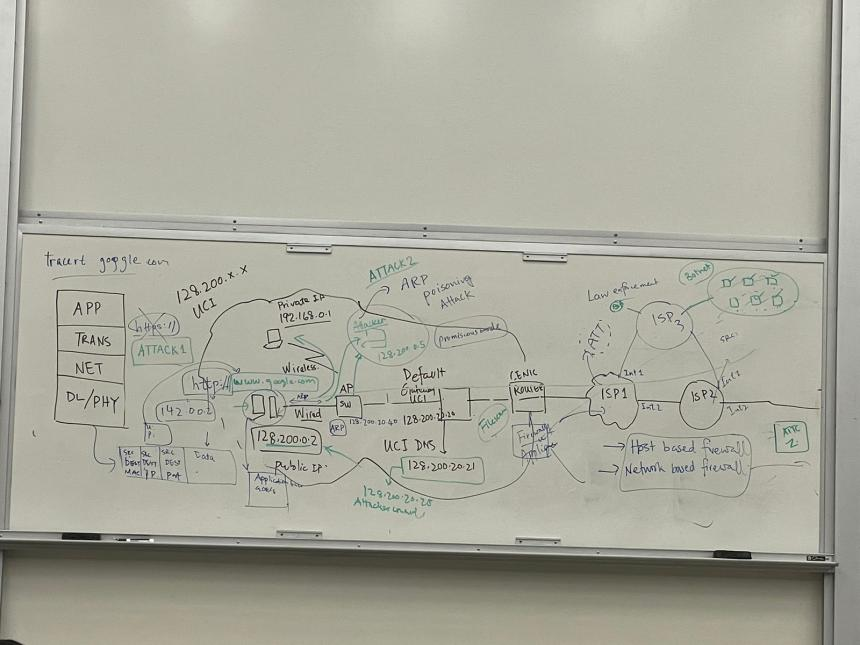
Application Layer Protocols

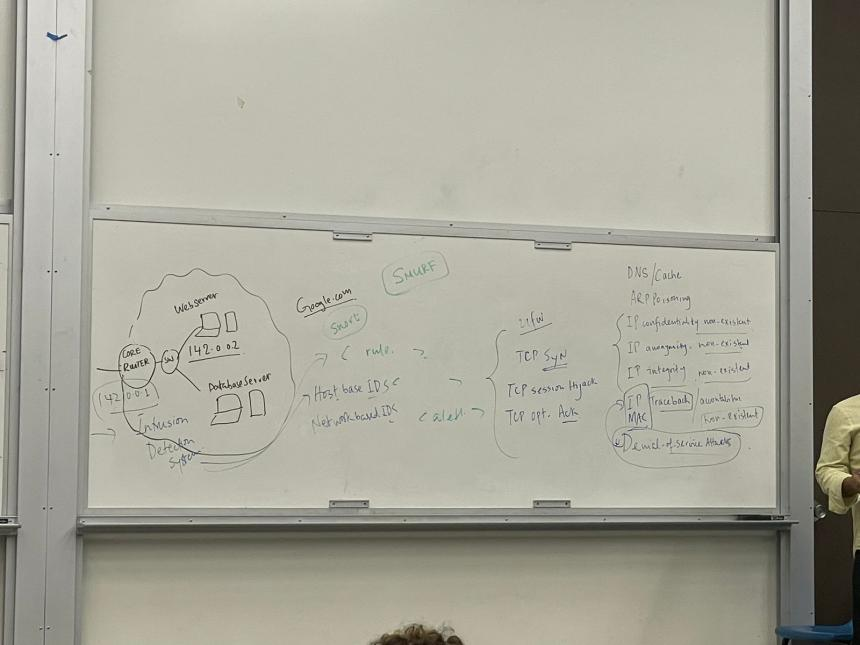
resolves domain name to ip address

SSH (Secure Shell) for remote access to other computer

FTP (File Transfer Protocol) to share files between computers

TEXTBOOK NETWORK





Browser:

check if you have access to the website you typed in by the hash/cache?

get the IP address and dns at Default Gateway

**DNS/Cache Attack**

1. modify local cache to connect to malicious website/computer
2. modify dns to go to a malicious computer

fix

IP address must maintain its integrity

ARP

using ARP protocol to translate IP addresses into MAC addresses.

**ARP Poisoning Attack**

a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table.

Problem with IP

**IP Confidentiality**

IP packets can be looked at in plaintext when passing ip packet without SSL

**IP anonymity**??

**IP MAC Integrity**??

**IP Traceback** not existing

send a fake ip packet and no way to traceback where it was sent from

Smurf Attack (Fraggle attack uses UDP protocol instead)

sending internet control message protocol (ICMP) packets and cause denial of service (**DDoS**)

TCP Session Hijacking

an authorized user gains access to a legitimate connection of another client in the network. The attacker can read and modify transmitted data packets, as well as send their own requests to the addressee.

TCP OPT. attack

ddos ⇐ increasing the number of requests ⇐ sending fake packets

Routering

ISP1 (interface …)

ISP2

collect data from customer packets

Line Router

gets the address of the website

Application Layer HTTP, NNTP, Telnet, FTP, and so on

Transport Layer Security TLS

Transmission Control Protocol TCP

Internet Layer IP

Packet-filtering firewalls in ISP

filters IP packets based on source and destination IP address, and source and destination port (if the source port doesn’t match IP address, drop the packet)

* ISP has the lookup table to get IP address by source port
* network based firewall and host based firewall

(Proxy firewalls

acts as a gateway between internal users and the internet. Proxies = gateway applications used to route internet and web access from within a firewall)

IDS = Intrusion detection system

detect suspicious activities → generates alerts for a security operations center (SOC) for further investigation/actions/remediation

also has host-based and network-based system

### TLS

Network Protocol Stack ⇒ interconnectivity rules for a layered network model such as in the OSI or TCP/IP models.

Confidential Issue: anyone sitting between the users and web server can see the data to be sent, such as UCI router, ISP and Google Core Router

Fix: HTTPS (application level) = HTTP owns SSL/TLS:

1. Get IP/Do TCP Handshake
2. Google sends its digital certificates. Google public key signed by a certified authority’s private key
3. UCI computer browser verifies the certificate with CA’s public key pre-installed
4. UCI drop browser extracts the Google web servers public key from the digital certificate

If someone interrupts the progress, and sends the user a previous digital certificate of Google server ⇒ the attacker don’t have google’s private key, so the data is not vulnerable

1. UCI browser creates a symmetric session key encrypts with Google public key and send to Google server
2. Google server use its own private key to decrypt the symmetric key

Anonymous Issue: anyone in between know what user is sending to what server

* many Denial Of Service is very difficult to avoid in networking scenarios

### Virtual Private Network

VPN allows users to create a secure, private network over a public network by:

physical NIC (network interface card) ⇒ create virtual NIC by authentication in an encrypted process with UCI public key ⇒ traffic through UCI will use virtual NIC and other ones will use physical NIC (because UCI don’t allow access outside of the UCI to limit traffic?)

Way 1 to secure

* VPN client website needs to check HTTPS to ensure the website is not putting a malicious public key, and directing the user to send data to a malicious computer
* Encrypted public key with VPN (UCI.edu)
* Encrypt symmetric session key using VPN public key
* VPN server decrypts using VPN private key

Way 2 to secure (IPSec)

* Use IPSec to encrypt data packet sending from Google Server and only can see the ip address of the destination IPSec ⇒ no one can view the data
* The user has no control over the IPSec.
* Add IPSec between TCP and IP. APP → TCP → IPSec → IP → PHY/DL
* It’s basically wrapping the whole data packet with a new ip header
* Works for servers who have multiple servers in different locations

Encrypted process has two methods

IPSec Tunneling

Utilizes the Internet Protocol Security protocol

IPSec has a mode called Tunneling mode, where the original IP packet is encapsulated and placed into a new IP packet

TLS/SSL Tunneling

Tunneling done outside the kernel, at the application level

Idea is to put each VPN-bound IP packet inside a TCP or UDP packet

The other end of the tunnel will extract the IP packet from the TCP/UDP payload

To secure the packets, both ends will use TLS/SSL protocol on top of TCP/UDP

### Symmetric Encryption

Def

plaintext - original message

ciphertext – hidden/coded message

cipher (encryption)- algorithm for transforming plaintext to ciphertext

encipher (encrypt) - converting plaintext to ciphertext

decipher (decrypt) - recovering plaintext from ciphertext

key - info used in cipher known only to sender/receiver

cryptography - study of encryption principles/methods

cryptanalysis (code breaking without knowing key) - study of principles/ methods of deciphering ciphertext

#### Technique

Substitution - each element is mapped into another element

Transposition/Permutation - elements are rearranged

#### Classic cipher: based on either substitution or transposition

Caesar cipher (shift by k letters)

c = E(k, p) = (p+k) mod 26

p = D(k, c) = (c-k) mod 26

vulnerable to cryptanalytic attack or brute-force attack for only 26 possible ciphers

Monoalphabetic cipher (map to random letter)

pattern in a language can be used for cryptanalytic attack (most common/rare letter, most frequently used letter after the common letter…)

Vigenere cipher

simplest polyalphabetic substitution cipher

shift each element at i position with the given shift Ki

Ex.

plaintext: aabcd

key: bcdef

ciphertext: bcegi

the language nature can be hidden in ciphertext

vulnerable when the attacker know the length of the key

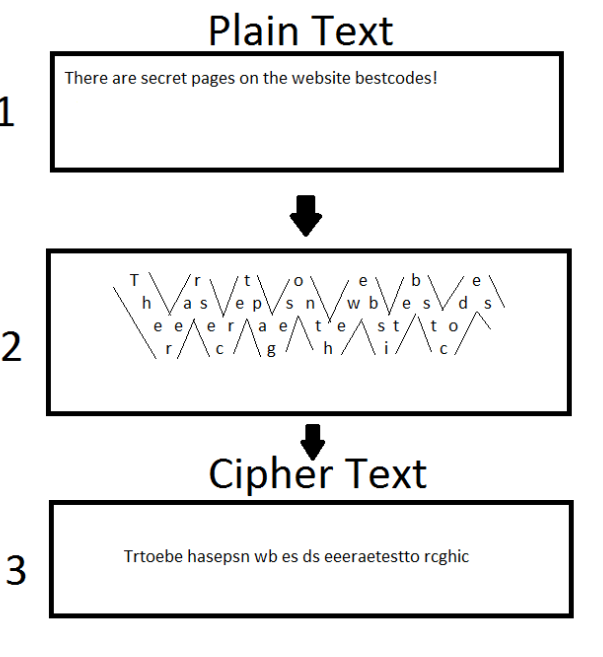
One-time pad

truly random key if len(key) = len(message)

unbreakable if used once

problem with generation and safe distribution of key

Rail Fence cipher (Transposition cipher)



#### Modern cipher: based on combination of substitution and transposition

Block cipher process plaintext one block of elements at a time (ex. AES)

Stream cipher processes input continuously (ex. RC4) there is a limit for input size

* MOD
* XOR used in encryptions (modern?). important when dealing with different language systems

A = 41 = 0100 0001

B = 42 = 0100 0010

AB = **0100 0001 0100 0010** plaintext

key=4 = 0110 0110 0110 0110

XOR = 0010 0111 0010 0100 ciphertext encrypted

key=4 = 0110 0110 0110 0110

XOR = **0100 0001 0100 0010** plaintext decrypted

(use the block of encrypted ciphertext as the next key)

AB = **0100 0001 0100 0010** plaintext

key = 0110 0010 0011 0111

XOR = 0010 0011 0111 0101 ciphertext encrypted

key=4 = 0110

XOR = **0100 0001 0100 0010** plaintext decrypted

### AES Encryption

#### Rijndael

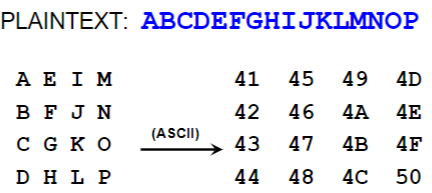
128/192/256 bit key = 9/11/13 rounds (larger key ⇒ more rounds ⇒ safer cipher)

128 bit plaintext

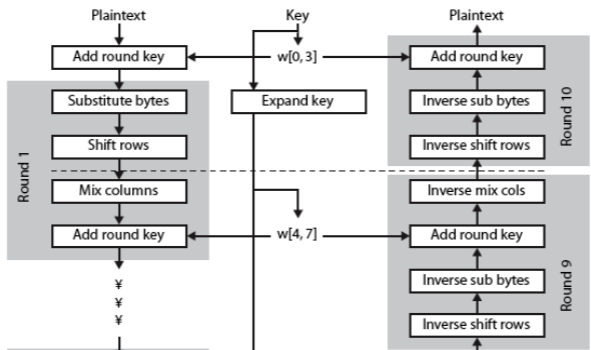
operates on entire block in every round

data block of 4x4 is state

Ex.



In each round, SP Network is applied



byte substitution (1-S box entry used on each byte)

given a lookup table and the current byte, find the result by current byte as row and column

shift rows (column permutation)

1st unchanged

2nd left shift by 1 byte

3rd left shift by 2 byte

4th left shift by 3 byte

mix columns (row permutation)

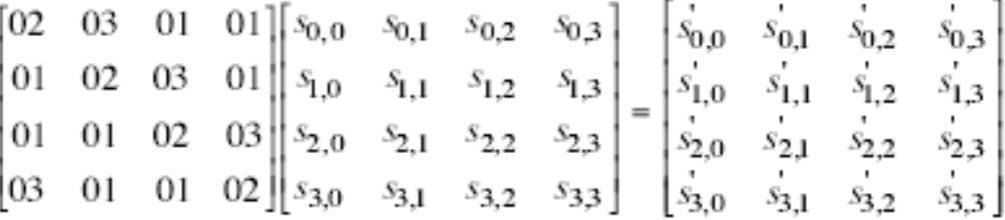
each column is processed separately

each byte is replaced by a value dependent on all 4 bytes in that column

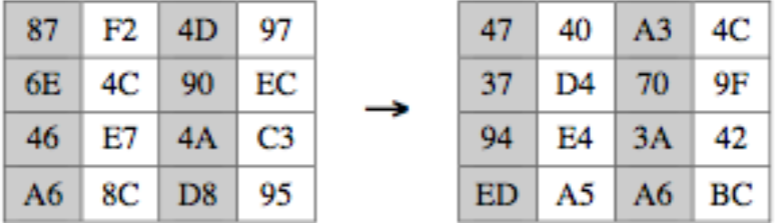
addition is XOR

a \* 0x02 = shift left by one. If leftmost bit = 1 before shift, result must apply XOR 0x1B

a \* 0x03 = (a \* 0x02) XOR (a \* 0x01)



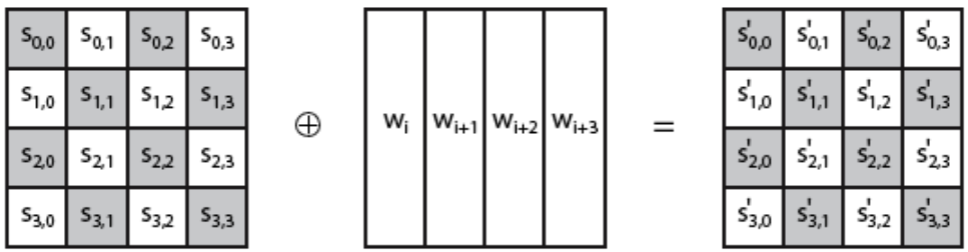
Ex. table A



47 = (87 \* 02) XOR (6E \* 03) XOR (46) XOR (A6)

37 = first column in A \* second row (01 02 03 01)

add round key



replace value with old value XOR the value in round key table with the same position

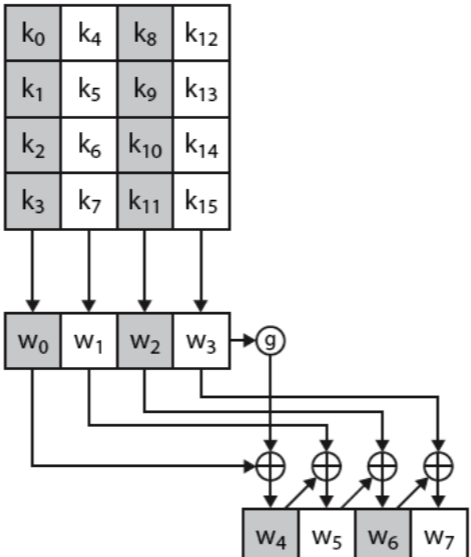
* after 9 or more rounds, the final round does NOT include mix column

#### AES Key Expansion

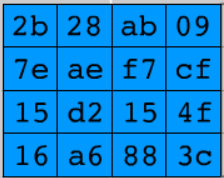
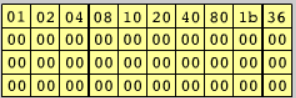
expand 128-bit key to 44/52/60 32-bit words

start by copying key into first 4 words

then loop creating new words based on previous words



Ex.

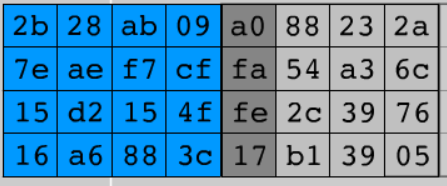
with Rcon

Round 1

1st column: 09 cf 4f 3c → up shift by 1 → Substitute with s-box → XOR 2b 7e 15 16 XOR **01 00 00 00** → a0 fa fe 17

2nd column: a0 fa fe 17 XOR 28 ae d2 a6 = 88 54 2c b1

…



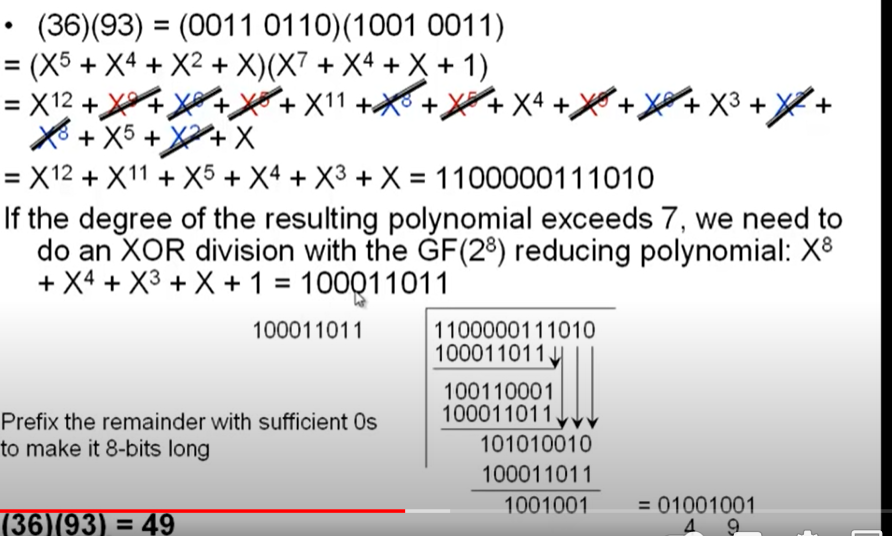
Round 2

1st column: 2a 6c 76 05 → up shift by 1 → substitute → XOR a0 fa fe 17 XOR **20 00 00 00** → f2 c2 95 f2

…

Do until Rcon is used up

#### AES Arithmetic



Ex. Integers {..-2,-1,0, 1, 2} for operation +

Associative?

Additive identity?

Additive inverse?

Ex. {-1,0,½,1,2} Multiplicative identity

Zn when n is not prime ⇒ 1 exists in the table because a\*b mod n ⇒ problem that multiplicative inverse doesn’t exist in the result table ⇒ the key will not be able to encrypt/decrypt symmetrically

* when mod is used, prime number usually required?

Finite Fields

Galois Fields

Def

Galois Fields for every prime power there is a unique finite field containing elements.

When p = 1, it’s primitive galois fields,

When p > 1, it’s extension galois fields (only when p=2, XOR will work)

Extension fields. Some can be expressed in reducible polynomial

max(degree of A(x)) = n-1 for

An element of gf(pn) can be represented as a polynomial A(x) with highest degree n-1 and coefficients in gf(p) i.e {0,..p-1}

Ex. gf(2) = {0,1} so only 0 or 1 as coefficients ⇒ the element appears or not

gf(2^2) = {0, 1, x, x+1} ⇒ elements = {0,1,2,3}

Ex.

Irreducible: can’t be factored into another polynomials of smaller degree

x2+1 is irreducible but x2-1= (x-1) (x+1) is

Modulus for multiplication: irreducible polynomial

• The job of the irreducible polynomial is to chop down the degree greater than n-1

AES Multiplication

2=010=x

when multiplying by 2 ⇒ highest degrees increase by 1 and needs to chop down by XOR the reducible polynomial A(x)

### Secure Communication

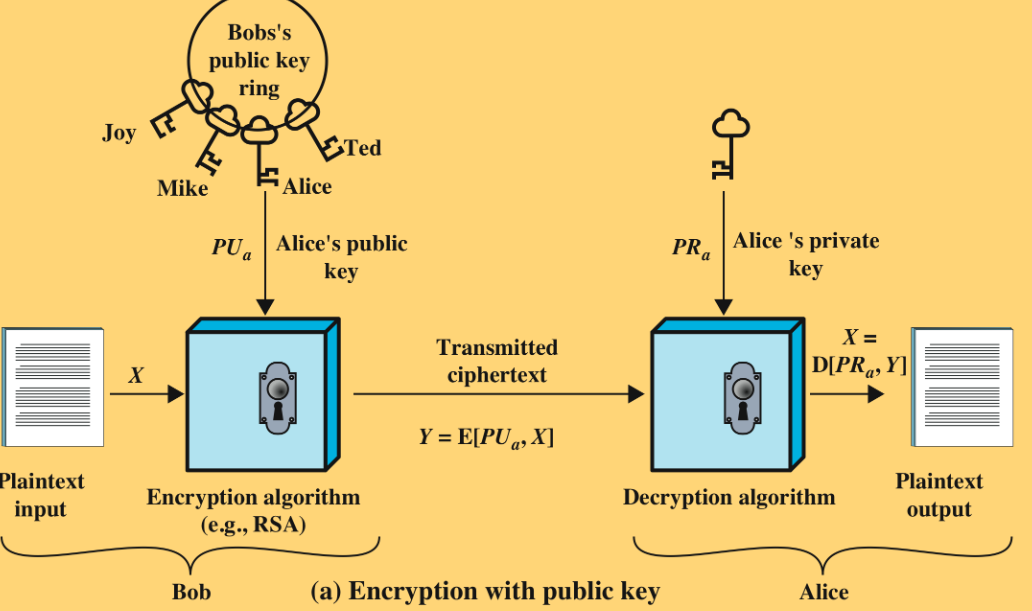
**digital certificate** ⇒ exchange public key, symmetric session key.

key distribution – how to have secure communications in general without having to trust a KDC with your key

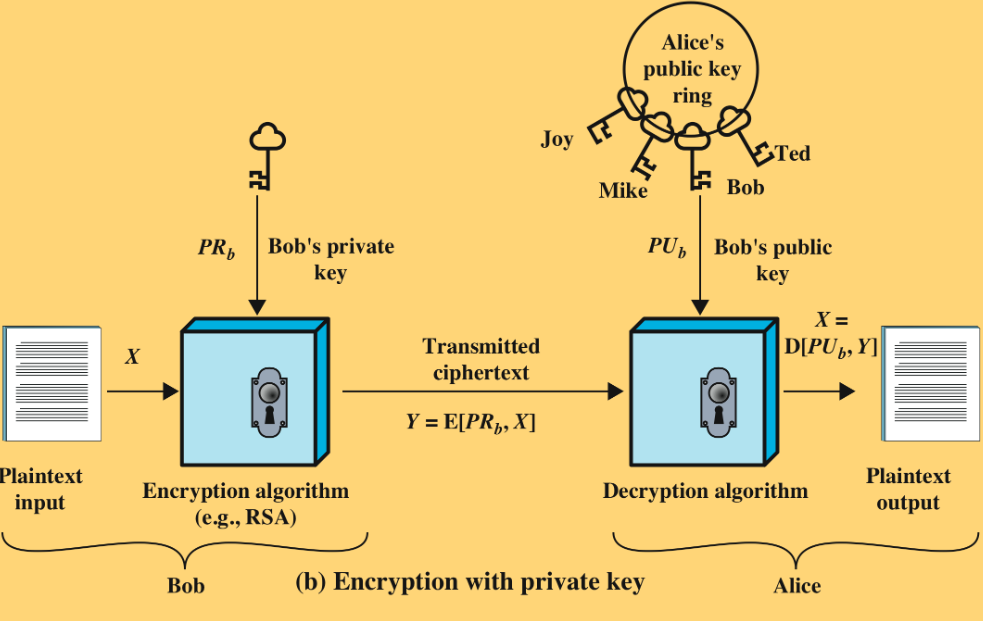
–digital signatures – how to verify a message comes intact from the claimed sender

Public key application

encryption/decryption (confidential)



digital signature (authorization)



key exchange of session keys (session keys)

RSA Key Generation

| select p,q  calculate n = p \* q  calculate  select integer e  calculate d  public key  private key | p and q both prime, p != q    KU = {e,**n**} (not )  KR = {d,**n**} |
| --- | --- |

* since n is very big, it’s hard to reverse-engineer
* e can be small because exponentiation is expensive
* AES key is much faster

For encryption

plaintext: M<n

ciphertext:

For decryption

ciphertext: C

plaintext:

**ARS algorithm on the RSAAlgorithmWithExample**

Ex. Step 1 key generation

p=17 and q=11

n=17\*11=187

select e such that e is relatively prime to and e < 160; we choose e=7

determine d such that de mod 160 = 1 and d < 160. The correct value is d=23

Ex. Step 2 encryption decryption

plaintext 88 ⇒ 88 mod 187 = 11

#### Division Algorithm

if divide a by n get integer quotient q and integer remainder r such that:

a = qn + r where 0 <= r < n;

remainder r often referred to as a residue

Ex.

a = 11, n=7 11 mod 7 = 4

11 = 7\*1 + 4 r=4, q=1

a = -11, n=7 11 mod 7 = 3

-11 = 7\*(-2)+3 r=3, q=-2

a=-4, n=11 -4 mod 11 =7

-4=11\*(-1)+7 r=7, q=-1

Euclid Algorithm for greatest common divisor

def gcd(a, b):

while b:

a, b = b, a % b

return a

Ex. gcd(22,60) = gcd(60,22)

60=22\*2+16

22=16\*1+6

16=6\*2+4

6=4\*1+**2** = gcd

4=**2**\*2+0

Euclid + Bizout Algorithm

Ex. if gcd is 1, we can reverse the process???

11 = 8(1) + 3

8 = 3(2) + 2

3 = 2(1) + 1

2 = 1(2)

1 = 3 − 2(1)

1 = 3 − (8 − 3(2))(1) = 3 − (8 − (3(2)) = 3(3) − 8

1 = (11 − 8(1))(3) − 8 = 11(3) − 8(4) = 11(3) + 8(−4)

⇒ 3-(-4) = 7

Residue system -4 mod 11 = 7

Modular inverse of 8 mod 11 = 7

Ex. what is the inverse of 10 module 17

17 = 10 + 7

10 = 7 + 3

7 = 3\*2 + 1

1 = 7 - 3\*2

1 = 7 - (10-7)\*2 = 7\*3 - 10\*2

1 = (17-10)\*3 - 10 \* 2

1 = 17\*3 - 10\*5

⇒ 17 - 5 = 12

#### Euler Totient Function

Def

when doing arithmetic modulo n

complete set of residues is: 0..n-1

reduced set of residues is those numbers (residues) which are relatively prime to n

eg for n=10, complete set of residues is {0,1,2,3,4,5,6,7,8,9} reduced set of residues is {1,3,7,9}

Function

p is prime ⇒ ø(p)=p-1

p.q (p,q rel prime) ⇒ ø(p\*q)=ø(p) \* ø(q)

Ex. ø(37) = 36, ø(21)= ø(3.7) = (3–1)x(7–1) = 2x6 = 12

#### Fermat’s theorem

Ex. a=2, p=3, 2^2 mod 3=1

#### Euler’s Theorem

a generalization of Fermat's Theorem

Ex.

a=3; n=10; ø(10)=4 ⇒

a=2;n=11; ø(11)=10 ⇒

Ex. Why RSA Works

⇐ Euler’s Theorem

in RSA, n = p\*q, …

by euler’s theorem,

### Final Review

**Nov 28**

2.

1 = 138\*12 + (-5)\*331

gcd(a,b) = ax+by = 1, multiplicative inverse of 12 mod 331 is 138 (12\*138 mod 331 = 1)

-5 is multiplicative inverse of 331 mod **12**. **(-5+12=7 if it’s negative MOD 12 to make it positive)**. 7 \* 331 mod 12 = 1

3. not sure why

Nov 16

1. check the result

**Nov 2**

Oct12

For CAs (Certificate Authorities), CA generates a digital certificate, digitally signs it with its private key.

D. forward secrecy - making sure to use different session keys