Usage Of Cryptography

Moshe Kravchik
Credits: Mark Stamp

Agenda

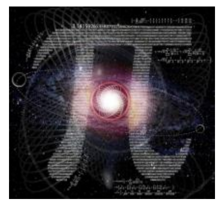
- History of Cryptography
- Symmetric Encryption
- Asymmetric Crypto
- MACs and hash functions
- Digital signatures
- Certificates and PKI


https://flic.kr/p/6keSjR

Introduction → Usage of crypto → Crypto in context → Authentication & Authorization → Vulnerabilities and Defensive Programming → OS Security concepts → Network Security concepts → Designing Secure Systems → Human Factor

Why do we need crypto

- Complex math!
- The core technology of cyberspace
  - Secret communication
  - Data confidentiality
  - Data integrity
  - Authentication
  - E-Commerce
  - Digital currency …



https://flic.kr/p/brdXxC

3

History of Cryptography

- Egypt, China
- אתב"ש בספר ירמיהו
- A cipher or cryptosystem is used to encrypt the plaintext
- The result of encryption is ciphertext
- We decrypt ciphertext to recover plaintext

4

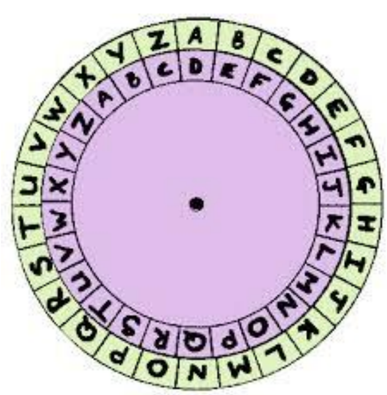
Key

- Need strong cipher
  - Need many different strong ciphers!
  - How to make someone to forget the cipher?
- A key is used to configure a cryptosystem

5

Caesar and its attacks

- The simplest substitution cipher
- What is the key?
- How to break it?
- How to make it stronger?



Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

6

Substitution cyphers and attacks

- Shift by n for some n in {0,1,2,…,25}
- Then key is n
- Example: key n = 7

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

hello → OLSSV

7

Cryptanalysis I: Try Them All

- A simple substitution (shift by n) is used
- But the key is unknown
- Given ciphertext: XIVQMREXIH
- How to find the key?
- Only 26 possible keys - try them all!
- Exhaustive key search (brute force)
- Solution: key is n = 4

1: whuplqdwhg
2: vgtokpcvgf
3: ufsnjobufe
4: terminated
5: sdqlhm`sdc

8

Least-Simple Simple Substitution

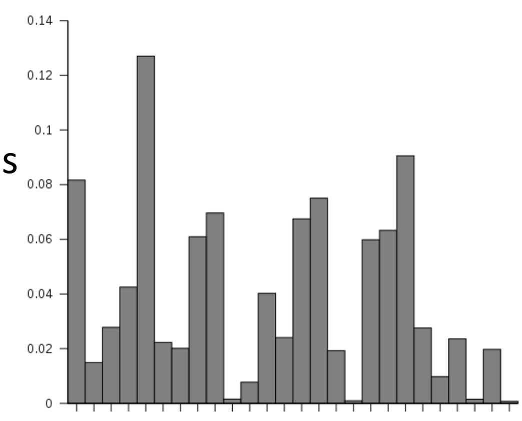
- In general, simple substitution key can be any permutation of letters
- Not necessarily a shift of the alphabet
- Then 26! > 2^{88} possible keys!
- A superfast computer testing 2^{40} per second would take 8.900.000 years…

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	J	I	C	A	X	S	E	Y	V	D	K	W	B	Q	T	Z	R	H	F	M	P	N	U	L	G	O

9

Cryptanalysis II

- Letter frequency analysis
- Letter combinations frequency
- Words frequency
- Huge key space != stronger cipher!



10

Types of crypto attacks

- Cipher text only (Caesar)
- Known plaintext (Enigma, RC4)
- Chosen plaintext
- Chosen ciphertext
- Kerckhoffs (1883) Algorithm can't stay secret (Enigma, A5, DVD, US Navy)
  – Security through obscurity

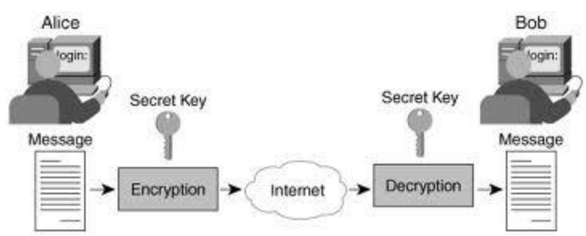

Radiation at B-52 Crash Site
Los Angeles Times
FINAL
U.S. SHIPS HEADING FOR NORTH KOREA
U.S. Strength Low in Crisis Area

Claude Shannon

- The founder of Information Theory
- 1949 paper: Communication Theory of Secrecy Systems
- Fundamental concepts
  – **Confusion** - obscure relationship between plaintext and ciphertext
  – **Diffusion** - spread plaintext statistics through the ciphertext
- Proved that one-time pad is unbreakable

Symmetric encryption

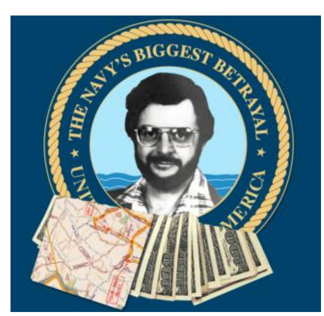
- Symmetric algorithm – the same key used for decryption and encryption
- All encryption algorithms used to be symmetric …



13

Modern symmetric encryption

- Translates the bytes of plaintext into ciphertext
- DES, 3-DES and now AES are standard symmetric encryption algorithms
- Problem – key distribution (n*n keys for n pairs)
- Problem – key management
- Problem – non-repudiation



14

Asymmetric crypto

- Motivation: solve the key distribution problem
  - Secure banking online
- Secret communication without agreed shared key!
- **Some operations are easy to do in one direction, but hard to do in the reverse direction**
  - Scrambling an egg vs. undoing it*
  - Insulting a person vs. making him/her forget it*
  - Closing a padlock vs. opening it

*Credits to Yaron Sella for this example

Asymmetric crypto

- Asymmetrical mathematical problems:
  - Assigning values to variables vs. solving equations
  - Multiplying numbers vs. factoring (7919 *6967 = 55171673)(RSA)
  - Discrete Log (Diffie Hellman)
  - You'll learn how they work in other courses!
- Modular calculus

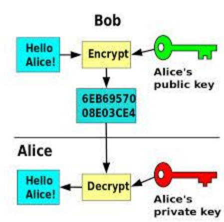
  8 + 5 mod 12 = 13 mod 12 = 1

Public and Private Keys

- A user generates a pair of keys: public and private.
- Public is published to the whole world and is used for encryption
- Private is secret and is used for decryption
- It is hard to get the private key from the public
- Public key cryptography is very slow , used to pass a symmetric session key

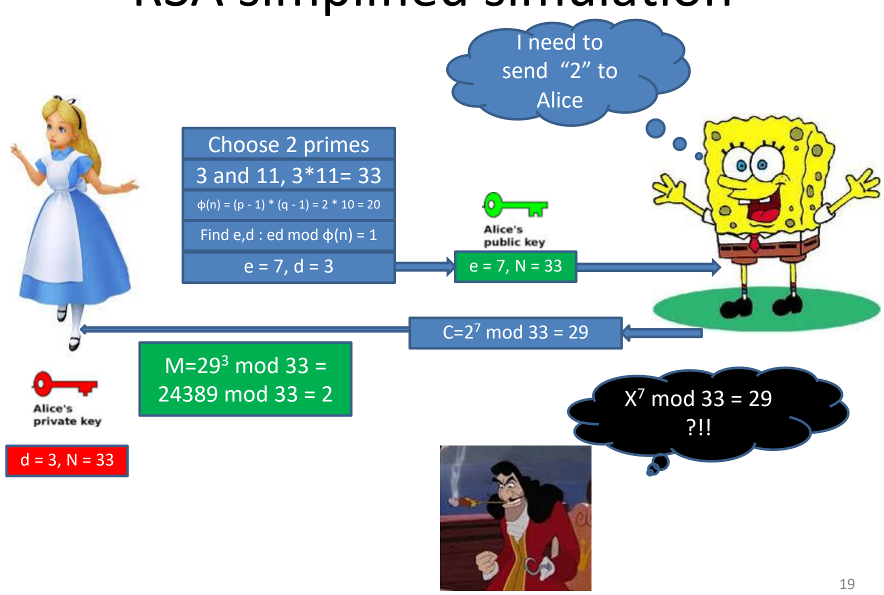
$C = M^e \bmod N$

$M = C^d \bmod N$



18

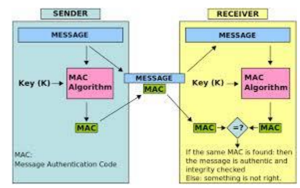
RSA simplified simulation



19

Message Authentication Code (MAC)

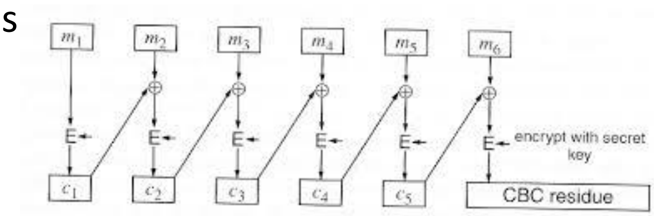
- Why do we need it?
- A number added to a message
- Uses a shared secret key
- Authentication and Integrity (no confidentiality)



20

Message Authentication Code (MAC)

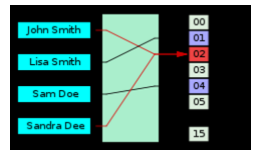
- Example – last block of AES-CBC encryption
- Any change in the plaintext must result in a different MAC!
- Can't fake the message for the given MAC
- Based on block cipher symmetric encryption and hashes



21

One Way Hash Functions

- Hash function: maps a large object to a small fingerprint (e.g. length of string, first character)
  - Many collisions
  - Data $X = (X_0,X_1,X_2,\ldots,X_{n-1})$, each X_i is a byte
  - Define $h(X) = X_0+X_1+X_2+\ldots+X_{n-1}$
  - Is this a secure cryptographic hash?

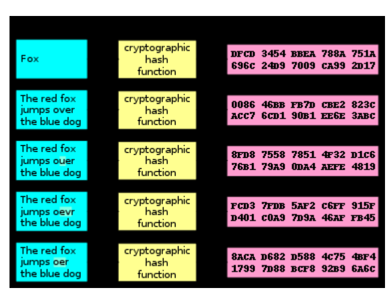


- Cryptographic hash functions practically uninvertible:
  - Easy to compute
  - Infeasible to find a message given a hash (preimage)
  - Infeasible to change the message without changing hash
  - Infeasible to find two messages with the same hash (collision resistance)

22

One Way Hash Functions

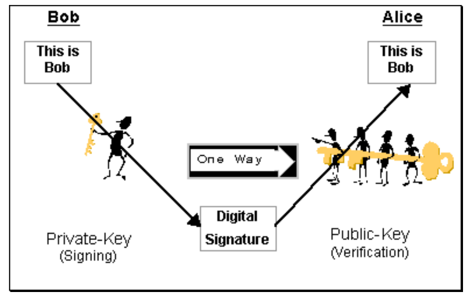
- Provide integrity (no key!)
- Hashed MAC (HMAC) – uses a key to provide also authentication
- Widely used: software packages, firmware updates, digital signatures…
- SHA (1 - deprecated, 256), MD5 – also deprecated, [see here why]



23

Digital signatures

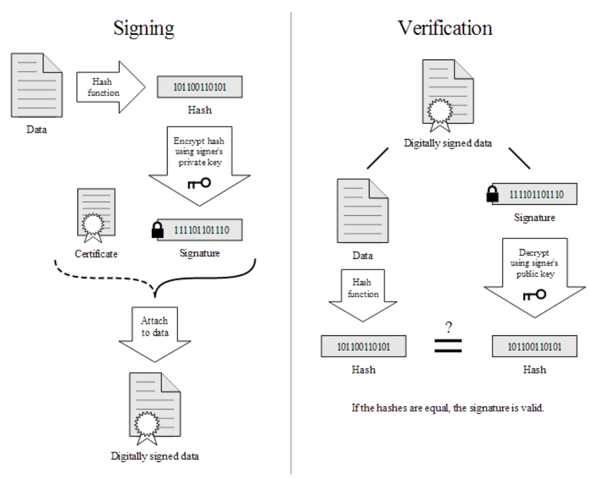
- Using the private key for encryption uniquely authenticates the sender
- Everyone can verify that Alice sent this message-signature
- Can't be reused for another message
- Can prove it was Alice who sent the message (unlike in shared secret schemes)



24

Digital signing

- Authentication + integrity
- RSA
- DSA
- Used in: secure mail, official documents, software images, certificates, …



25

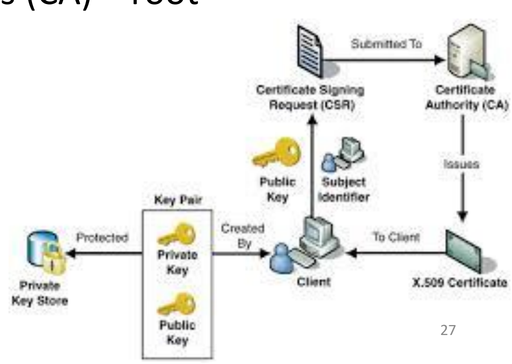
Certificates

- Where all public keys are kept?
- What guarantees that this is indeed Alice's public key?
- Certificate:
  - Credentials (name, organization, email)
  - Public key
  - Signed by someone you trust
    - Chain Of Trust
- X.509 is the standard format

26

Public Key Infrastructure

- In real life we need lots of certificates, who will sign all of them?
- A small amount of trusted Certificates Authorities (CA) – root CAs
- Root CA's public keys are preinstalled



27

PKI challenges

- Is the name enough? (Think of a phone book)
- How does the CA verifies trustfulness of the applicant?
- What makes CA trusted
  - Stolen CA private keys
- Key revocation handling (CRL)
- Can we trust the code that verifies that the certificate content is correct?

28

29

Terms learnt

- Cipher, plaintext, ciphertext
- Key
- Cryptanalysis
- Brute force
- Confusion, diffusion

- Symmetric and asymmetric crypto
- Public and private key
- MAC, one way hash, HMAC
- Digital signatures
- PKI

Summary

- Cryptography helps with Confidentiality and Integrity
- Classic crypto is easy to understand and break
- Symmetric ciphers are fast, but keys are a mess
- Asymmetric crypto solves the key management problem
- Digital signatures provide authentication and integrity