CSE 484 / CSE M 584: Computer Security and Privacy

# Cryptography [Intro]

Spring 2017

Franziska (Franzi) Roesner franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

#### **Vulnerability Analysis and Disclosure**

- What do you do if you've found a security problem in a real system?
- Say
  - A commercial website?
  - UW grade database?
  - Boeing 787?
  - TSA procedures?

# Abj sbe fbzr pelcgbtencul!

Now for some cryptography!

#### **Cryptography and Security**

- Art and science of protecting our information.
  - Keeping it **confidential**, if we want privacy.
  - Protecting its **integrity**, if we want to avoid forgeries.







Images from Wikipedia and Barnes & Noble

#### Some Thoughts About Cryptography

- Cryptography only one small piece of a larger system
- Must protect entire system
  - Physical security
  - Operating system security
  - Network security
  - Users
  - Cryptography (following slides)
- Recall the weakest link



• Famous quote: "Those who think that cryptography can solve their problems don't understand cryptography and don't understand their problems."

#### Improved Security, Increased Risk

- RFIDs in car keys:
  - RFIDs in car keys make it harder to hotwire a car
  - Result: Car jackings increased

# 

- RFIDs in car keys:
  - RFIDs in car keys

#### Biometric car lock defeated by cutting off owner's finger

POSTED BY CORY DOCTOROW, MARCH 31, 2005 7:53 AM I PERMALINK

– Result: Car jackin Andrei sez, "'Malaysia car thieves steal finger.' This is what security visionaries Bruce Schneier and Ross Anderson have been warning about for a long time. Protect your \$75,000 Mercedes with biometrics and you risk losing whatever body part is required by the biometric mechanism."

> …[H]aving stripped the car, the thieves became frustrated when they wanted to restart it. They found they again could not bypass the immobiliser, which needs the owner's fingerprint to disarm it.

They stripped Mr Kumaran naked and left him by the side of the road - but not before cutting off the end of his index finger with a machete.

#### XKCD: http://xkcd.com/538/



#### **Alice and Bob**

• Archetypical characters



#### Received April 4, 1977



#### A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman\*

#### Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

- Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
- 2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

#### **Common Communication Security Goals**

#### **Privacy** of data:

Prevent exposure of information

#### **Integrity** of data:

Prevent modification of information



#### History

- Substitution Ciphers
   Caesar Cipher
- Transposition Ciphers
- Codebooks
- Machines
- Recommended Reading: **The Codebreakers** by David Kahn and **The Code Book** by Simon Singh.

#### History: Caesar Cipher (Shift Cipher)

 Plaintext letters are replaced with letters a fixed shift away in the alphabet.



- Example:
  - Plaintext: The quick brown fox jumps over the lazy dog
  - Key: Shift 3
    - ABCDEFGHIJKLMNOPQRSTUVWXYZ
    - DEFGHIJKLMNOPQRSTUVWXYZABC
  - Ciphertext: wkhtx lfneu rzqir amxps vryhu wkhod cbgrj

#### History: Caesar Cipher (Shift Cipher)

- ROT13: shift 13 (encryption and decryption are symmetric)
- What is the key space?
   26 possible shifts.
- How to attack shift ciphers?
  Brute force.



#### **History: Substitution Cipher**

- Superset of shift ciphers: each letter is substituted for another one.
- Add a secret key
- Example:
  - Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Cipher: **ZEBRASCDFGHIJKLMNOPQTUVWXY**
- "State of the art" for thousands of years

#### **History: Substitution Cipher**

Rigrams

- What is the key space? 26! ~= 2^88
- How to attack?





th	1.52%	en	0.55%		ng	0.18%
he	1.28%	ed	0.53%		of	0.16%
in	0.94%	to	0.52%		al	0.09%
er	0.94%	it	0.50%		de	0.09%
an	0.82%	ou	0.50%		se	0.08%
re	0.68%	ea	0.47%		le	0.08%
nd	0.63%	hi	0.46%		sa	0.06%
at	0.59%	is	0.46%		si	0.05%
on	0.57%	or	0.43%		ar	0.04%
nt	0.56%	ti	0.34%		ve	0.04%
ha	0.56%	as	0.33%		ra	0.04%
es	0.56%	te	0.27%		ld	0.02%
st	0.55%	et	0.19%		ur	0.02%
Trigrams:						
1.	the	6.ion		11.	nce	
2.	and	7.tio		12.	edt	
3.	tha	8.for		13.	tis	
4.	ent	9. nde		14.	oft	
5.	ing	10.has		15.	sth	

#### **History: Enigma Machine**

Uses rotors (substitution cipher) that change position after each key.





Key = initial setting of rotors

Key space? 26<sup>n</sup> for n rotors

#### **Kerckhoff's Principle**

- Security of a cryptographic object should depend only on the secrecy of the secret (private) key.
- Security should not depend on the secrecy of the algorithm itself.

#### How Cryptosystems Work Today

- Layered approach:
  - Cryptographic primitives, like block ciphers, stream ciphers, hash functions, and one-way trapdoor permutations
  - Cryptographic protocols, like CBC mode encryption, CTR mode encryption, HMAC message authentication
- Public algorithms (Kerckhoff's Principle)
- Security proofs based on assumptions (not this course)
- Don't roll your own!

### Flavors of Cryptography

• Symmetric cryptography

Both communicating parties have access to a shared random string K, called the key.

- Asymmetric cryptography
  - Each party creates a public key pk and a secret key sk.

#### Symmetric Setting

Both communicating parties have access to a shared random string K, called the key.



#### **Asymmetric Setting**

Each party creates a public key pk and a secret key sk.



# Achieving Privacy (Symmetric)

Encryption schemes: A tool for protecting privacy.



### Achieving Privacy (Asymmetric)

Encryption schemes: A tool for protecting privacy.



### Flavors of Cryptography

• Symmetric cryptography

Both communicating parties have access to a shared random string K, called the key.

- Asymmetric cryptography
  - Each party creates a public key pk and a secret key sk.

# Flavors of Cryptography

- Symmetric cryptography
  - Both communicating parties have access to a shared random string K, called the key.
  - Challenge: How do you privately share a key?
- Asymmetric cryptography
  - Each party creates a public key pk and a secret key sk.
  - Challenge: How do you validate a public key?

# Confidentiality: Basic Problem

Given: both parties already know the same secret.

<u>Goal</u>: send a message confidentially.

How is this achieved in practice?

Any communication system that aims to guarantee confidentiality must solve this problem.

#### **One-Time Pad**



Cipher achieves perfect secrecy if and only if there are as many possible keys as possible plaintexts, and every key is equally likely (Claude Shannon, 1949)

#### **Advantages of One-Time Pad**

- Easy to compute
  - Encryption and decryption are the same operation
  - Bitwise XOR is very cheap to compute
- As secure as theoretically possible
  - Given a ciphertext, all plaintexts are equally likely, regardless of attacker's computational resources
  - ... <u>as long as</u> the key sequence is truly random
    - True randomness is expensive to obtain in large quantities
  - ... <u>as long as</u> each key is same length as plaintext
    - But how does sender communicate the key to receiver?

#### **Problems with One-Time Pad**

- Key must be as long as the plaintext

   Impractical in most realistic scenarios
   Still used for diplomatic and intelligence traffic
- Insecure if keys are reused

#### **Dangers of Reuse**



Learn relationship between plaintexts  $C1 \oplus C_2 = (P1 \oplus K) \oplus (P_2 \oplus K) =$  $(P1 \oplus P_2) \oplus (K \oplus K) = P1 \oplus P_2$ 

#### **Problems with One-Time Pad**

- Key must be as long as the plaintext
  - Impractical in most realistic scenarios
  - Still used for diplomatic and intelligence traffic
- Insecure if keys are reused
  - Attacker can obtain XOR of plaintexts

#### **Integrity**?



#### **Problems with One-Time Pad**

- Key must be as long as the plaintext
  - Impractical in most realistic scenarios
  - Still used for diplomatic and intelligence traffic
- Insecure if keys are reused
   Attacker can obtain XOR of plaintexts
- Does not guarantee integrity
  - One-time pad only guarantees confidentiality
  - Attacker cannot recover plaintext, but can easily change it to something else

### **Reducing Key Size**

- What to do when it is infeasible to pre-share huge random keys?
  - When one-time pad is unrealistic...
- Use special cryptographic primitives: block ciphers, stream ciphers
  - Single key can be re-used (with some restrictions)
  - Not as theoretically secure as one-time pad