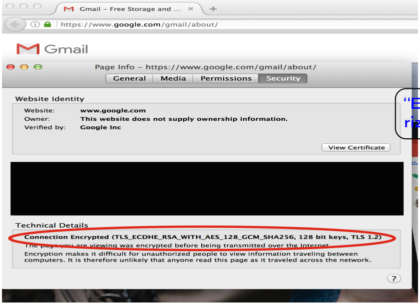
Lecture 1: Introduction

Instructor: Omkant Pandey

Spring 2017 (CSE 594)

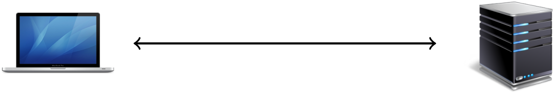
Cryptography

- Most of us rely on cryptography everyday
  - Online banking
  - Ordering something on Amazon
  - Sending emails
  - Interacting on social media...
- Your browser often tells you what it is using:



"Encryption makes it difficult for unauthorized people to view the information"

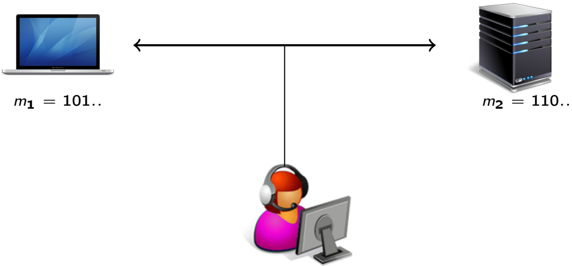
Secret Communication



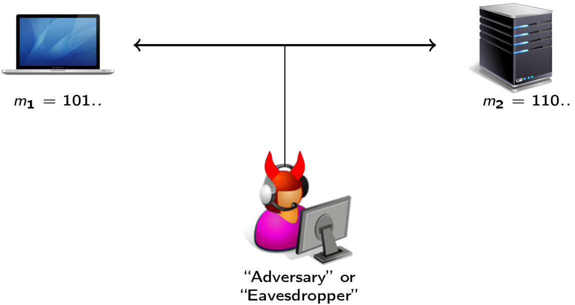
Secret Communication

Secret Communication

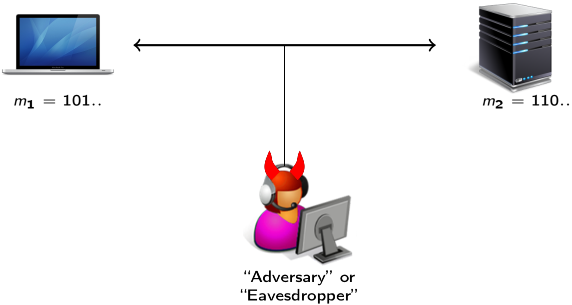
Secret Communication



Secret Communication



Secret Communication



- Historically, such mechanisms are called ciphers.

Ciphers

k 

 k

Ciphers

k   k

$m = 101..$

Ciphers

k 

$m = 101..$

$E(k, m)$

 k

Ciphers

k 

 k

$m = 101..$

$E(k, m) \rightarrow c$

Ciphers

k  $\xrightarrow{c}$  k

$m = 101..$

$E(k, m) \rightarrow c$

Ciphers

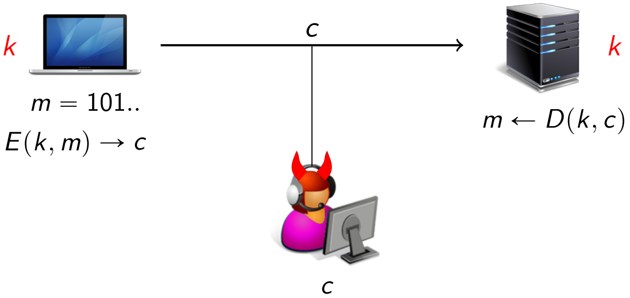
k  $\xrightarrow{\quad c \quad}$  k

$m = 101..$

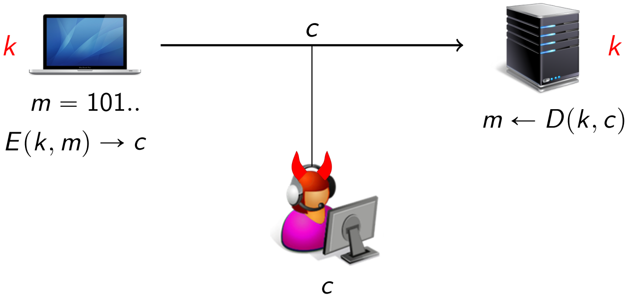
$E(k, m) \rightarrow c$

$m \leftarrow D(k, c)$

Ciphers

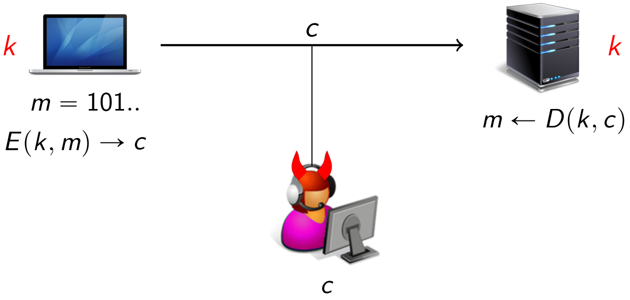


Ciphers



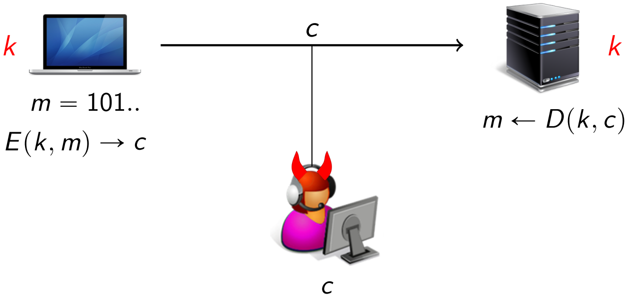
- E, D are called encryption and decryption algorithms, and k, the secret key.

Ciphers



- E, D are called encryption and decryption algorithms, and k, the secret key.
- E could be randomized, so that c changes every time!

Ciphers



- E, D are called encryption and decryption algorithms, and k, the secret key.
- E could be randomized, so that c changes every time!
- Symmetric Cipher: k is same for both E and D.

Historical Ciphers

...all completely broken

Caesar Cipher

- Named after Julius Caesar who used it to communicate with his generals.
- You simply **shift** your alphabets by a fixed number...
  - Shift by 1: letter A becomes B, B becomes C, ... Z becomes A.
  - Shift by any amount $k = 1, 2, \ldots, 25$.
  - Decrypt by shifting back...
  - Example: encrypt ATTACK with Shift 1 = BUUBDL.
- Breaking Caesar Cipher:
  - Brute force: try all 26 possible shifts.
  - Visible patterns and letter frequencies:

    ATTACK = BUUBDL and DEFEND = EFGFOE
- Ciphertext only attack! (worst kind)

Substitution Cipher

- Choose a **random permutation** of English alphabets...
- $\{A \to T, B \to L, C \to K, \ldots, Z \to H\}$ (no repeating)
- Encrypt: just map plaintext letters according to the substitiution (key)
- Decrypt: revert back using the same key
- Cannot break by brute forcing for the key:

  $\#$ possible keys $= 26! \approx 2^{88}$
- Break by frequency analysis

Frequency Analysis

- Frequency of letters, bigrams, double letters in English:

Letters								
e	t	a	o	i	n	s	r	h
12.49%	9.28%	8.04%	7.64%	7.57%	7.23%	6.51%	6.28%	5.05%

Bigrams											
th	he	in	er	an	re	on	at	en	nd	ti	es
3.56%	3.08%	2.43%	2.05%	1.99%	1.85%	1.76%	1.49%	1.45%	1.35%	1.34%	1.34%

Double Letters										
ll	ss	ee	oo	tt	ff	pp	rr	mm	cc	nn
0.58%	0.41%	0.38%	0.21%	0.17%	0.15%	0.14%	0.12%	0.10%	0.08%	0.07%

- Breaking substitution cipher (ciphertext only attack):
  - Collect a long ciphertext – frequency patterns will not change.
  - Compute frequencies of various letters
  - Reconstruct the key: most frequent letter represents "E", second most is "T", etc. Use bigrams, trigrams, etc. for more.
  - Great blogpost about this: http://norvig.com/mayzner.html

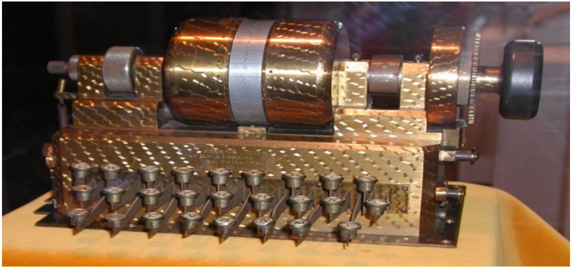
(Image courtesy Rick Wicklin: blog.sas.org)

Vigenère Cipher

- Use a random keyword to shift. Repeat to match length.
- Keyword = CAB
- Alphabets in an array of length 26: A=0, B=1, C=2,. . ., Z=25.
- Shift for the keyword CAB = 201.
  - HELLO (message)
  - CABCA (repeated key to match the length)
  - JEMNO (ciphertext)
  - H→J, E→E, L→M, L→N, O→O
- Again, easily broken by frequency analysis: guess key length and analyze frequencies.
- Ciphertext only attack!

Rotor Machines

- After the typewriter, encryption based on rotor machines.



The Hebern Machine (Wikipedia)

 - Rotor encodes the key
 - Typed symbol encrypted with the next symbol on the rotor
 - Rotor moves as you type, changing the key each time.
 - Measure the cycle after which the key starts repeating

Rotor Machines

- Machines with more rotors, more rotors = bigger key space.

Enigma with 3 rotors (Wikipedia)

- More rotors = more keys $\approx 2^{36}$ in Enigma with 3-rotors.
- All susceptible to known cryptanalysis methods
- Friedman had several important cryptanalysis methods for Hebern.
- Further improved and highly optimized by others.
- Turing designed a machine to search for Enigma key from known ciphertexts/plaintext pairs.

Digital Age

- Data Encryption Standard (DES), designed by IBM in response to government's call for a good encryption standard, in 1974.
- DES has roughly 2^{56} keys, not considered safe with today's computing powers.

- Advanced Encryption Standard (AES):
  - Designed by Vincent Rijmen and Joan Daemen (originally called Rijndael) in 1998.
  - Selected and standardized by the US government through intense competition
  - Comes with different key sizes and other parameters (typical for such ciphers)
- Many other ciphers known today, e.g., Salsa, Twofish, ...

Today

- Design of such symmetric ciphers is an ongoing process
- Ciphers such AES are not yet (publicly known to be) broken
- Replaced with new parameters (or ciphers altogether) as weaknesses are discovered
- Rigorous process for selecting new ciphers

- These ciphers are quite fast and practical to use. Practical applications will always rely on them as the main method.

- A different approach to designing ciphers:
  - Take cryptanalysis "out of the equation"...
  - Design ciphers that are provably hard to break!
  - Possible to do; drawback: slow speed (practical but not as fast as say AES).

Beyond Secret Communication

- We will do a detailed study of encryption schemes that allow secret communication.
- Cryptography can do a lot more than secure communication.
  - Digital Signatures
  - Digital Cash
  - Electronic voting
  - Zero Knowledge Proofs
  - Coin flipping over internet
  - Secure multiparty computation
  - Verifiable Computation
  - ...
- **Provable security approach: strive for constructions that are mathematically proven hard to break.**

Cryptography as a rigorous science

- Understand what you want to do: functionality
- Who are you protecting against, and what: threat model
- Propose a construction
- Prove that breaking your construction is:
  - either impossible, or
  - at least as hard as solving some known "hard problem"

Next class

- What does it mean for a cipher to be secure?
- Shannon's treatment of perfect secrecy.