University of Colorado **Boulder**

CSCI 3403 INTRO TO CYBERSECURITY

Lecture: 2-2

Topic: Cryptography

Presenter: Matt Niemiec

Announcements

- 新年快乐
- Don’t forget about Wal-Mart talk next Tuesday
  - Details on next slide
  - Talk to Nolen Scaife for more details
- Much of the today’s lecture is borrowed from Matt Bishop’s “Introduction to Computer Security”
- Please submit your groups by 1/31/20
  - https://bit.ly/2G11c1G to submit your group

JERRY GEISLER

Chief Information Security Officer

at

Walmart

INDUSTRY LEADER FOCUSED ON BEST-IN-CLASS INFORMATION SECURITY PRACTICES, INNOVATION AND BUSINESS ENABLEMENT

TUESDAY, JANUARY 28

12:30-1:45 PM

ECCR 150

ANYBODY IS WELCOME!

WALMART IS #1 ON FORBES FORTUNE 500 LIST

LEARN ABOUT THEIR AMAZING CYBERSECURITY PROGRAM

Technology, Cybersecurity and Policy Program

UNIVERSITY OF COLORADO **BOULDER**

Cryptography

What is Cryptography?

- We kind of know what it is...
- Can anyone give a definition?
- NOT the solution to all security problems

Types of Cryptography

1) Symmetric key encryption
2) Public/private key encryption
3) Hashing (one-way encryption)

Vocab

- Plaintext
- Encryption/decryption algorithm
- Secret key
- Ciphertext

Attack Vocab

- Brute force vs. cryptanalysis
- Types of cryptanalytic attacks
  - Ciphertext only
  - Known plaintext
  - Chosen plaintext/ciphertext
  - Man-in-the-middle
  - Side channel
  - Birthday attacks
- These all use weaknesses in the algorithm design

Symmetric Encryption

Symmetric Encryption

- Already discussed briefly in week 1
- Encryption key == Decryption key
- Requires sender and receiver to have same key

Decode the words from your spelling list using the secret code. Write your answer in the space provided.

CODE	q	w	e	r	t	y	u	i	o	p	a	s	d	f	g	h	j	k	l	z	x	c	v	b	n	m
LETTER	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

1. stdgf ____________
2. kqwwoz ____________
3. ixfudn ____________
4. ygktlz ____________
5. usqll ____________

Image source: http://www.brailleauthority.org

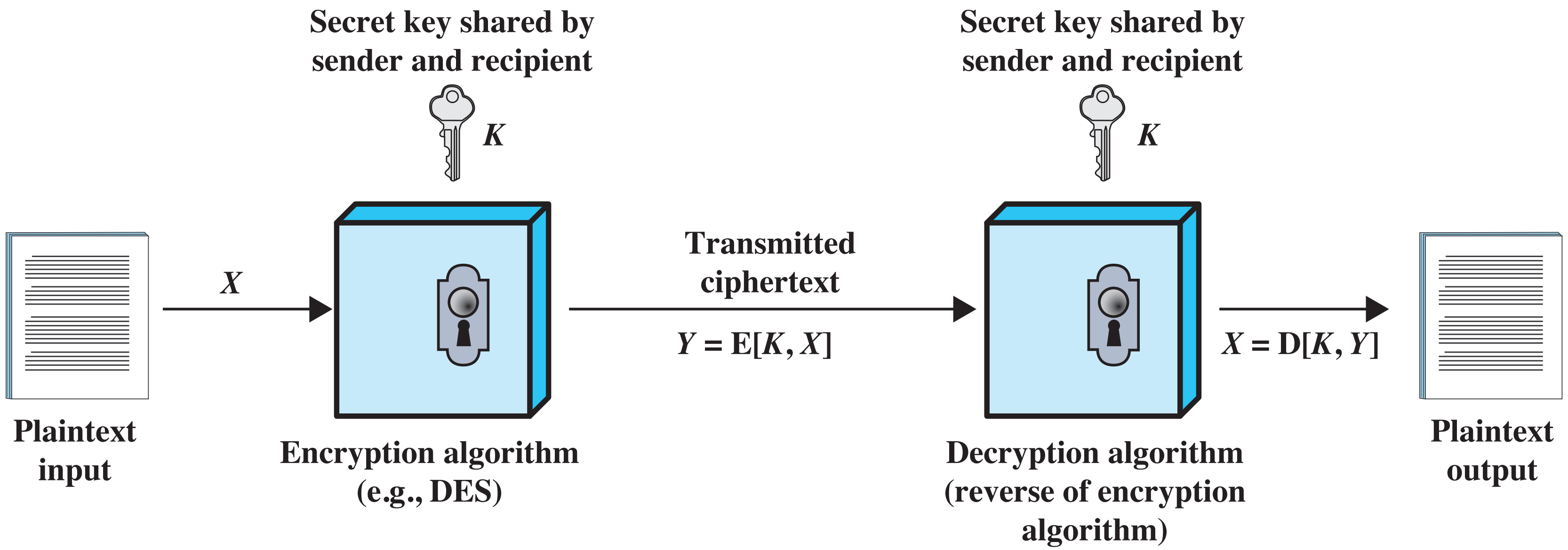

Figure 2.1 Simplified Model of Symmetric Encryption

Example: Caesar Cipher

- Key is a number between 1 and 25
- “Rotate” the character that many times
- Let K=3
  - Plaintext = “HELLO WORLD”
- Caesar Cipher a type of substitution cipher

Problems: Caesar Cipher

- Ciphertext: “qcbtwrsbhwoz hslh”
  - Break it!

Improvement: Vigènere Cipher

- Caesar Cipher, but the key is a phrase
- Repeat key when out of characters
- Let K="abcde"
  - Encrypt "HELLO WORLD"

Problems: Vigènere Cipher

- What's wrong here?

Improvement: One-Time Pad

- Completely random string
- Use only once
- Key is at least as long as the message
- Can XOR if working with bits

Problems: One-Time Pad

- What's wrong with THAT?!

Cryptanalysis

Brute Force Caesar Cipher

- Try every single key
- Break: “KHOOR ZRUOG”
- https://cryptii.com/pipes/caesar-cipher

Cryptanalysis of Caesar Cipher

- Take advantage of weakness in English
- Some letters more common

1) Decrypt message with every key
2) For each letter, multiply frequency by probability of occurring
3) Sum over all previous numbers. Yields arbitrary number
4) The highest number is most likely the key

Character Frequencies

a	0.080	h	0.060	n	0.070	t	0.090
b	0.015	i	0.065	o	0.080	u	0.030
c	0.030	j	0.005	p	0.020	v	0.010
d	0.040	k	0.005	q	0.002	w	0.015
e	0.130	l	0.035	r	0.065	x	0.005
f	0.020	m	0.030	s	0.060	y	0.020
g	0.015					z	0.002

Statistical Analysis

- $f(c)$ frequency of character c in ciphertext
- $\varphi(i)$ correlation of frequency of letters in ciphertext with corresponding letters in English, assuming key is i
- $p(x)$ is frequency of character x in English

- *Formula:* $\varphi(i) = \Sigma_{0 \leq c \leq 25} f(c)p(c - i)$

Statistical Analysis, Cont.

- Do the math!
- Plug in i for all 26 possible keys
- $\varphi(i) = 0.1p(6 - i) + 0.1p(7 - i) + 0.1p(10 - i) + 0.3p(14 - i) + 0.2p(17 - i) + 0.1p(20 - i) + 0.1p(25 - i)$

Correlation: $\varphi(i)$ for $0 \le i \le 25$

i	$\varphi(i)$	i	$\varphi(i)$	i	$\varphi(i)$	i	$\varphi(i)$
0	0.0482	7	0.0442	13	0.0520	19	0.0315
1	0.0364	8	0.0202	14	0.0535	20	0.0302
2	0.0410	9	0.0267	15	0.0226	21	0.0517
3	0.0575	10	0.0635	16	0.0322	22	0.0380
4	0.0252	11	0.0262	17	0.0392	23	0.0370
5	0.0190	12	0.0325	18	0.0299	24	0.0316
6	0.0660					25	0.0430

The Result

- Most probable keys, based on φ:
  - $i = 6$, $\varphi(i) = 0.0660$
    - plaintext **EBIIL TLOLA**
  - $i = 10$, $\varphi(i) = 0.0635$
    - plaintext **AXEEH PHKEW**
  - $i = 3$, $\varphi(i) = 0.0575$
    - plaintext **HELLO WORLD**
  - $i = 14$, $\varphi(i) = 0.0535$
    - plaintext **WTAAD LDGAS**
- Only English phrase is for $i = 3$
  - That's the key (3 or 'D')

Cryptanalysis

- This is a simple example
- Cryptanalysis is extremely complex and math-heavy
- We can see how we'd use weaknesses
- We can see how longer texts would help the attacker

Modern Solutions

DES

- Invented in 1975
- Was most widely used until recently
- Algorithm has concerns
- Key length is 56 bits

Triple DES (3DES)

- Addresses large problem of small key
- Encrypt, decrypt, encrypt
- Provides backwards compatibility
- Sounds great!

Sweet32 Birthday Attack

- 3DES vulnerable because of small block size
- Discovery affected HTTPS, VPNs, etc.
- Requires hundreds of GBs of ciphertext
- NIST deprecated 3DES in 2017

Advanced Encryption Standard (AES)

Needed a replacement for 3DES

- 3DES was not reasonable for long term use

NIST called for proposals for a new AES in 1997

- Should have a security strength equal to or better than 3DES
- Significantly improved efficiency
- Symmetric block cipher
- 128 bit data and 128/192/256 bit keys

Selected Rijndael in November 2001

- Published as FIPS 197

Average Time to Break Key

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years

Block vs. Stream Ciphers

Block Cipher

- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common

Stream Cipher

- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key