

Flow

- 3 parts to Cryptography lecture in CSCI 415
- Intro to Cryptography → Symmetric Key Encryption → Asymmetric Key Encryption (digital signatures/ digital certificates/ digital envelopes) → SSL/ TLS
- 3 related lab components

Overview

- The fundamentals and history
- Character-Level Encryption
 - Substitution
 - Monoalphabetic
 - Polyalphabetic
 - Gronsfeld's System
 - Vigenere
 - Transpositional
- Bit-Level Encryption
 - Permutation
 - Exclusive OR (XOR)
 - Rotation
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm, Blowfish and RC5 (block ciphers)

Fundamentals

- Cryptography: process of converting plaintext (readable text) into ciphertext (unreadable/ encrypted text) by authorized sender - encryption
- Equally important is this system is the re-conversion from unreadable to readable text by authorized recipient – decryption
- Keys
- Symmetric Encryption
- Asymmetric encryption
- While cryptography obscures/ hides the meaning of the data from unauthorized user, it does not hide the data itself (what is that process called?)

History – cryptography is nothing new

- Egyptian hieroglyphics found on ancient monuments were encrypted (ca. 4500 BC)
- The Book of Jeremiah was written using a cipher, or key, known as atbash
- Connected with religious and academic literature and powers of the day (Queen Elizabeth I ca. 1550)
- Kama Sutra (ca. 2000 years ago) recommends that men and women learn the art of cryptography
- Julius Caesar: shifter letters by 3 positions (i.e. 'a' becomes 'd')
- Used both in WW I and WW II
- Good book: ["The Codebreakers"](#), David Kahn (McMillan, 1967)

War Machines

- Enigma machines used by Germans during WW II
- Developed by Arthur Scherbius
- How does it work?



The code was first broken by Polish cryptographers, then by the British and Americans

Enigma



Displayed at the National Cryptologic Museum

- 1) Commercial Enigma
- 2) Enigma T
- 3) Enigma G
- 4) Unidentified
- 5) Luftwaffe (Air Force) Enigma
- 6) Heer (Army) Enigma
- 7) Kriegsmarine (Naval) Enigma — M4.

Symmetric and Asymmetric Cryptography Algorithms

Type of Algorithm	Description
Symmetric	<ul style="list-style-type: none">▪ Uses a single key to encrypt and decrypt data▪ Both sender and receiver must agree on the key before the data is transmitted▪ Support confidentiality, but not authentication and nonrepudiation▪ Faster than asymmetric algorithms▪ Some difficulties??
Asymmetric	<ul style="list-style-type: none">▪ Uses 2 keys; one to encrypt and one to decrypt data▪ Support authentication and nonrepudiation▪ Slower than symmetric algorithms▪ Known as public key cryptography
Hashing	Algorithm used for verification Takes a variable-length input and converts it to a fixed-length output string called a hash-value

Article: <http://www.wired.com/news/technology/0,1282,32263,00.html>

Character-Level Encryption – Substitutional - Monoalphabetic

- Caesar's Cipher



Character-Level Encryption – Substitutional - Polyalphabetic

- Gronsfeld's System

Key: 7 3 4 1 7 3 4 1 7

Text: G R O N S F E L D

Crypto:

7 A E I M Q U Y

more secure

3 B F J N R V Z

4 C G K O S W

1 D H L P T X

Writing the letters out, row by row, and starting with the row having the lowest keyfigure gives the following unordered sequence:

DHLPTXBFJNRVZCGKOSWAEIMQUY

Key: 7 3 4 1 7 3 4 1 7

Text: G R O N S F E L D

Crypto:

Character-Level Encryption – Substitutional - Standard Vigenere Vigenere Table

Plaintext	A	T	T	A	C	K	A	T	M	I	D	N	I	G	H	T
Key Letter	S	E	C	U	R	I	T	Y	S	E	C	U	R	I	T	Y

Key Letter

Plaintext	A	T	T	A	C	K	A	T	M	I	D	N	I	G	H	T
Key Letter	S	E	C	U	R	I	T	Y	S	E	C	U	R	I	T	Y
Crypto	X															

- | | |
|---|-----------------------------|
| ■ | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| | BCDEFGHIJKLMNOPQRSTUVWXYZA |
| | CDEFGHIJKLMNOPQRSTUVWXYZAB |
| | DEFGHIJKLMNOPQRSTUVWXYZABC |
| | EFGHIJKLMNOPQRSTUVWXYZABCD |
| | FGHIJKLMNOPQRSTUVWXYZABCDE |
| | GHIJKLMNOPQRSTUVWXYZABCDEF |
| | HIJKLMNOPQRSTUVWXYZABCDEFG |
| | IJKLMNOPQRSTUVWXYZABCDEFGH |
| | JKLMNOPQRSTUVWXYZABCDEFGHI |
| | KLMNOPQRSTUVWXYZABCDEFGHIJ |
| | LMNOPQRSTUVWXYZABCDEFGHIJK |
| | MNOPQRSTUVWXYZABCDEFGHIJKL |
| | NOPQRSTUVWXYZABCDEFGHIJKLM |
| | OPQRSTUVWXYZABCDEFGHIJKLMNO |
| | PQRSTUVWXYZABCDEFGHIJKLMNO |
| | QRSTUVWXYZABCDEFGHIJKLMNO |
| | RSTUVWXYZABCDEFGHIJKLMNO |
| | STUVWXYZABCDEFGHIJKLMNO |
| | TUVWXYZABCDEFGHIJKLMNO |
| | UVWXYZABCDEFGHIJKLMNO |
| | VWXYZABCDEFGHIJKLMNO |
| | WXYZABCDEFGHIJKLMNO |
| | XYZABCDEFGHIJKLMNO |
| | YABCDEFGHIJKLMNO |
| | ZABCDEFGHIJKLMNO |

Character-Level Encryption – Substitutional -Vigenere

- Standard Vigenere was the main cryptographic system used by the Confederated States during the American Civil War, and four of the keyphrases used by the Confederates were:
 - **IN GOD WE TRUST**
 - **COMPLETE VICTORY**
 - **MANCHESTER BLUFF**
 - **COME RETRIBUTION**

The History of Codes and Ciphers in the United States prior to World War I

Character-Level Encryption – Substitutional - Unordered Vigenere

A table using a body consisting of a mixed sequence based on the keyword *SPHINX* could look like this

Plaintext	A	T	T	A	C	K	A	T	M	I	D	N	I	G	H	T
Key Letter	S	E	C	U	R	I	T	Y	S	E	C	U	R	I	T	Y

Key Letter

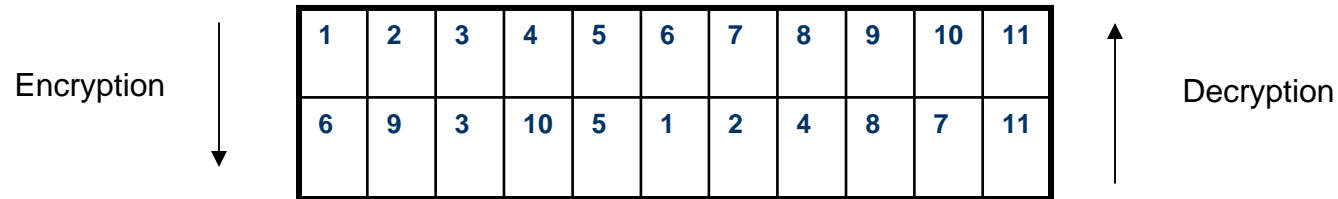
Plaintext	A	T	T	A	C	K	A	T	M	I	D	N	I	G	H	T
Key Letter	S	E	C	U	R	I	T	Y	S	E	C	U	R	I	T	Y
Crypto	N															

Plaintext

- | | |
|------------------------------|-----------------------------|
| SPHINX | ABCDEFGHIJKLMOQRTUVWYZ |
| PHINX | ABCDEFGHIJKLMOQRTUVWYZS |
| HINX | ABCDEFGHIJKLMOQRTUVWYZSP |
| INX | ABCDEFGHIJKLMOQRTUVWYZSPH |
| NX | ABCDEFGHIJKLMOQRTUVWYZSPHI |
| X | ABCDEFGHIJKLMOQRTUVWYZSPHIN |
| ABCDEFGHIJKLMOQRTUVWYZSPHINX | |
| BCDEFGJKLMOQRTUVWYZSPHINXA | |
| CDEFGJKLMOQRTUVWYZSPHINXAB | |
| DEFGJKLMOQRTUVWYZSPHINXABC | |
| EFGJKLMOQRTUVWYZSPHINXABCD | |
| FGJKLMOQRTUVWYZSPHINXABCDE | |
| GJKLMOQRTUVWYZSPHINXABCDEF | |
| JKLMOQRTUVWYZSPHINXABCDEFG | |
| KLMOQRTUVWYZSPHINXABCDEFGJ | |
| LMOQRTUVWYZSPHINXABCDEFGJK | |
| MOQRTUVWYZSPHINXABCDEFGJKL | |
| OQRTUVWYZSPHINXABCDEFGJKLM | |
| QRTUVWYZSPHINXABCDEFGJKLMO | |
| RTUVWYZSPHINXABCDEFGJKLMOQ | |
| TUVWYZSPHINXABCDEFGJKLMOQR | |
| UVWYZSPHINXABCDEFGJKLMOQRT | |
| VWYZSPHINXABCDEFGJKLMOQRTU | |
| WYZSPHINXABCDEFGJKLMOQRTUV | |
| YZSPHINXABCDEFGJKLMOQRTUVW | |
| ZSPHINXABCDEFGJKLMOQRTUVWY | |

Character-Level Encryption – Transpositional

- The Key defines which columns are swapped



1	2	3	4	5	6	7	8	9	10	11
a		g	o	o	d		g	o	o	d
f	r	i	e	n	d		i	s		
b	e	t	t	e	r		t	h	a	n
a		t	r	e	a	s	u	r	e	

plaintext

1	2	3	4	5	6	7	8	9	10	11
d										
d										
r										
a										

TRANSPOSE
Encryption Algorithm

Ciphertext

TRANSPOSE
Decryption Algorithm

1	2	3	4	5	6	7	8	9	10	11

Bit-Level Encryption – Exclusive OR (XOR)

- Opposite of biconditional: if two bits are same, then value is 0 and if they are different, then value is 1

sender

1	0	0	1	0	1	1	0
1	1	0	0	1	1	1	0

8-bit plaintext

KEY

8-bit ciphertext

receiver

1	1	0	0	1	1	1	0

8-bit ciphertext

KEY

8-bit plaintext

Bit-Level Encryption – Rotation

- Another way to encrypt a bit pattern is to rotate bits to the right or to the left. The key is the number of bits to be rotated

Plaintext

0	1	1	1	0	0	1	0
0	0	1	1	1	0	0	1

After 1 rotation

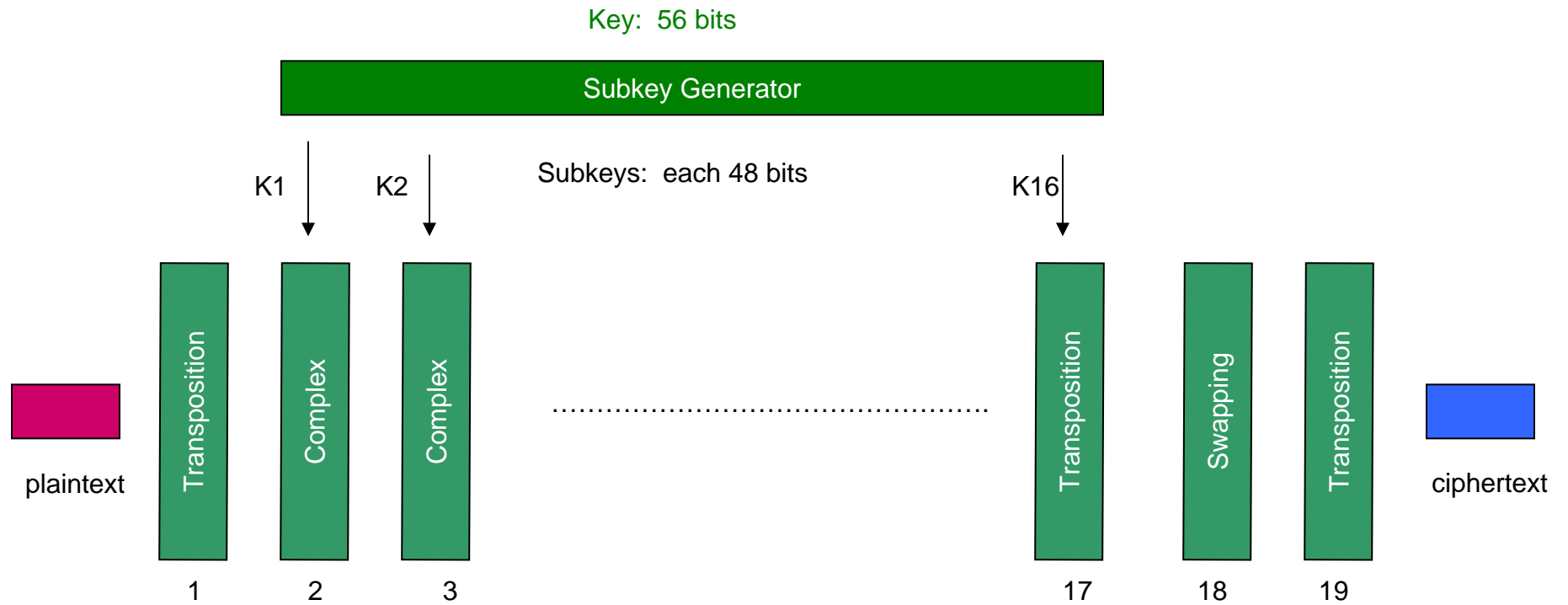
After 2 rotations

After 3 rotations

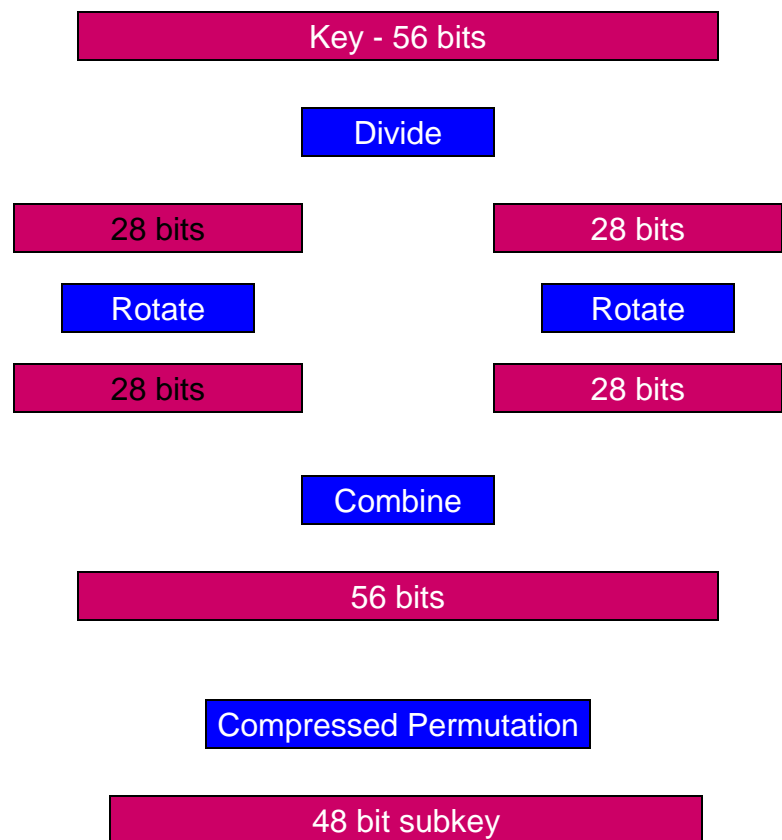
Data Encryption Standard (DES)

- National Security Agency (NSA) and National Institute of Standards and Technology (NIST) are responsible for the DES
 - NIST wanted a means of protecting sensitive but unclassified data. In the early '70s it invited vendors to submit data encryption algorithms
 - NIST accepted the already created Lucifer (IBM), but NSA modified it by reducing the key size from 128 bits to 64 bits and named it Data Encryption Algorithm (DEA) – not very original but...
- Was one of the most popular cryptographic algorithms
- Even though DES uses 64-bit encryption, only 56 bits are effectively used and 8 bits are used for parity
- DES is an example of bit-level encryption. Designed by IBM and adopted by the US government for nonmilitary and non classified use
- Encrypts a 64-bit plaintext, using a 56-bit key
- The text is put through 19 different and very complex procedures to create a 64-bit ciphertext
- The 56-bit key is no longer considered secure enough to be used – it has been broken in as little as 3.5 hours by fast computers
- DES is no longer the primary symmetric encryption algorithm and is no longer recommended for secure transmissions

Data Encryption Standard (DES)



Data Encryption Standard (DES) – Subkey Generation



Effective key length is 56 bits

4-bit key has 16 possibilities
56-bit key has 76 quadrillion possibilities
But parallel processing can guess keys

Advanced Encryption Standard (AES)



- The current standard used by the US government - replaces DES
- In 1997, NIST put out a request to the public for a new encryption standard
- National Institute of Standards and Technology (NIST) chose Rijndael symmetric algorithm as the basis of AES (October 2000)
 - The process began with the NIST publishing requirements for a new symmetric algorithm and requesting proposals
 - The requirements stated that the new algorithm had to be fast and function on older computers with 8-bit processors as well as 32 bit and 64 bit processors and be able to run on smart cards
 - After a lengthy process that required the cooperation of the US government, industry and higher education, 5 finalists were chosen and the ultimate winner was
 - the Rijndael algorithm from Belgians, Vincent Rijmen and Joan Daemen -
- 5 finalists: Rijndael, MARS, RC6, Serpent, Twofish
- AES – elegant mathematical formula, very fast execution
- AES uses 128-bit (performs 9 rounds), 192-bit (performs 11 rounds), and 256 bit keys (performs 13 rounds), ($1.1 * 10^{77}$ possible keys)
- Estimate time to crack: 149 trillion years – benchmarked by a machine cracking DES in 1 second (Universe is only about 20 billion years old)
- Other symmetric cryptography algorithms: IDEA (International Data Encryption Algorithm), Blowfish, RC5