



Applied Cryptography

Symmetric Key Cryptography



Learning Objectives

Upon completion of this unit:

- Students will be able to define *encryption*, *decryption*, *plaintext*, *ciphertext*, and *encryption/decryption key*, and explain their use in cryptography.
- Students will be able to describe attack scenarios against an encryption algorithm.
- Students will be able to use early cipher methods such as a Caesar cipher or substitution cipher to encrypt/decrypt data by hand.
- Students will be able to identify commonly used algorithms for symmetric encryption.
- Students will be able to explain the challenge of key distribution in symmetric key encryption.
- Students will be able to illustrate how symmetric key encryption works using software such as Kryptos.



Main Tenets of Information Security

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation



Cryptography

- Cryptography is “the practice and study of techniques for secure communication in the presence of adversaries” (Wikipedia)
- It is the science of designing systems to store and transmit data in a secure way so that it preserves its integrity and is accessible to only those with proper authentication and authorization.

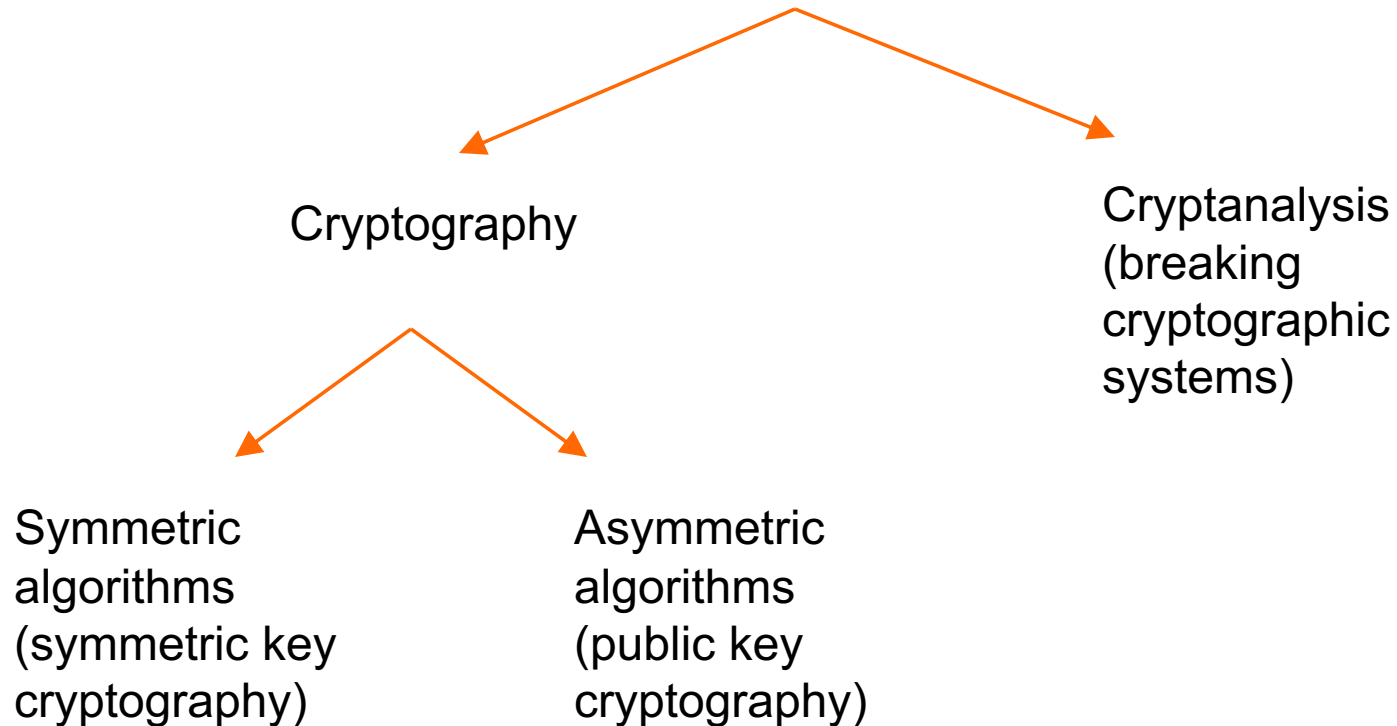


Cryptography and the Main Tenets of Information Security

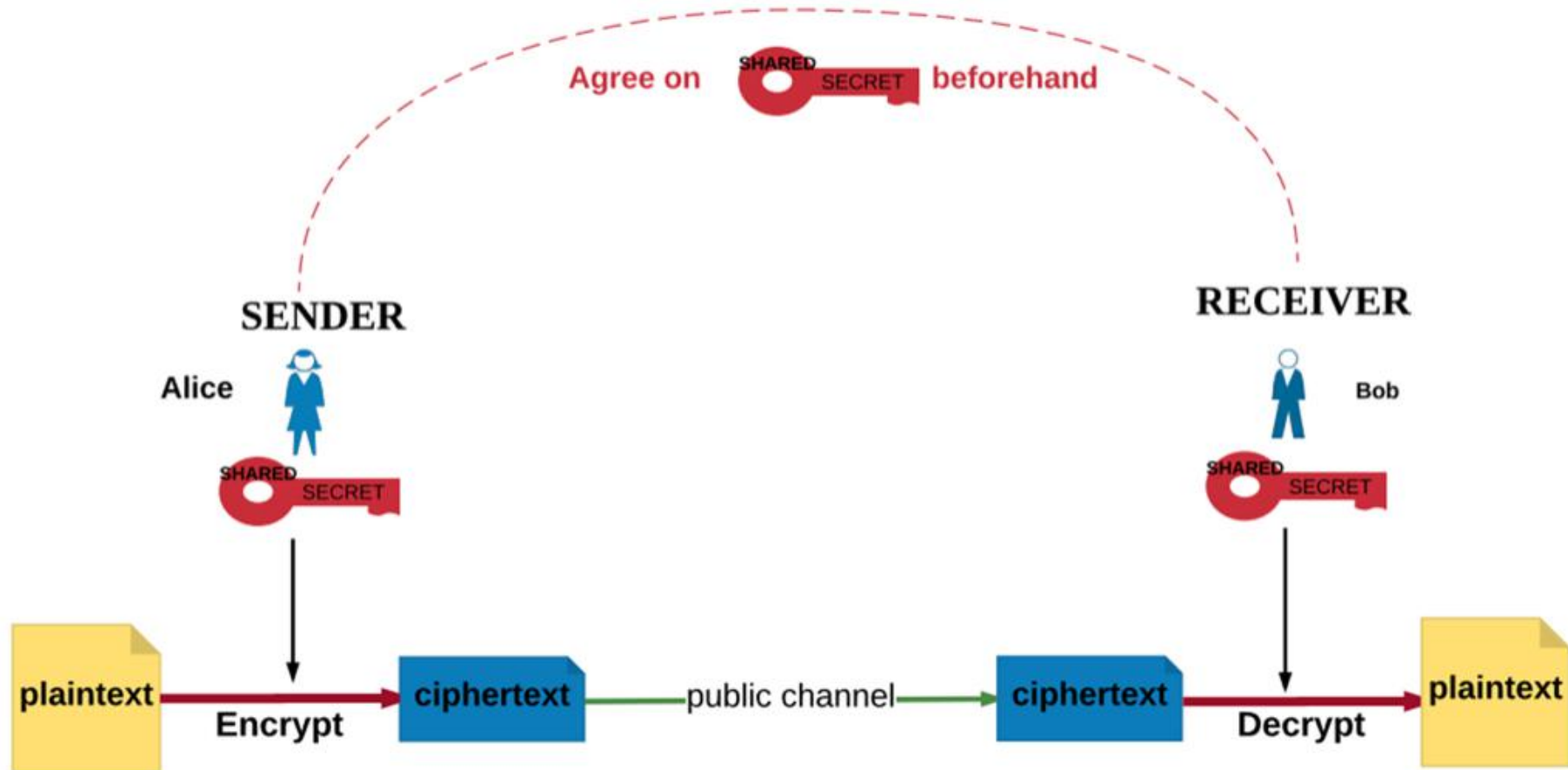
- Confidentiality
 - Encryption/decryption algorithms
- Integrity
 - Hash functions
- Authenticity
 - Digital signatures, digital certificates
- Non-repudiation
 - Digital signatures, digital certificates



Cryptology



Symmetric Key Cryptography



"Symmetric Encryption" by Yesem Kurt-Peker, licensed under [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)

A Simple Example of Symmetric Key Encryption: Caesar Cipher

- Shift each letter in the message 3 letters (to the right) in the alphabet.

Example:

plaintext: meet me after the toga party

ciphertext: PHHW PH DIWHU WKH WRJD SDUWB

Key=3

- If you know a ciphertext is obtained using the Caesar cipher, getting the original plaintext is simple!



Shift Cipher

- Generalization of the Caesar cipher
 - Shift each letter in the message k letters in the alphabet

Example with Key=11:

plaintext: meet me after the toga party
ciphertext: XPPE XP LQEPC ESP EZRL ALCEJ

- What would it take to break the shift cipher?
 - That is, if you know that a ciphertext is obtained using a shift cipher, how would you get the original plaintext?



Cryptanalysis of Shift Cipher

- Brute force approach: Try out all possible keys.
- What is the key space? How many keys are there?
 - For an English alphabet, there are 26. (Why?)
- Note that we assume here that the cryptanalyst knows the language that the original plaintext is in.



Kerckhoffs's Principle

- Auguste Kerckhoffs (1835-1903)
 - Dutch linguist and cryptographer
- A cryptosystem should be secure even if everything about the system, except the **key**, is public knowledge.
- Contrast “Security by obscurity” with Kerckhoffs's Principle.



Cryptanalysis of a Cipher

- Clearly state assumptions on what an attacker may have. Following Kerckhoffs's Principle, we assume that the details of the algorithm used for encryption is known. Does the attacker have
 - Ciphertext?
 - Pairs of plaintexts and ciphertexts?
 - The ability to choose any plaintext (and obtain the corresponding ciphertext) without knowledge of the key?
 - The ability to choose certain ciphertexts and get the corresponding plaintext without knowledge of the key?



Attack Scenarios on Ciphers

- **Ciphertext only attacks:** The attacker has only ciphertext(s).
- **Known plaintext attacks:** The attacker has ciphertext(s) and plaintext(s) for some of the ciphertexts.
- **Chosen plaintext attacks:** The attacker has ciphertexts and can choose a limited number of plaintexts and compute corresponding ciphertexts.
- **Chosen ciphertext attacks:** The attacker has the same ability as with chosen plaintext attacks, plus he/she can query a limited number of ciphertexts and get the plaintext for them.



Shift Cipher and Attack Scenarios

Task: Think about what it takes to decrypt a ciphertext that is obtained using the shift cipher under these scenarios:

- **Ciphertext only attacks** – How can you proceed to break the cipher if all you have is the ciphertext, GJFZYNKZQ IFD?
- **Known plaintext attacks** – You know that HELLO encrypts to MJQQT. Can you find the key?
- **Chosen plaintext attacks** – You have the opportunity to choose a plaintext and get its ciphertext (without knowing the key). What would you choose for the plaintext?
- **Chosen ciphertext attacks** – You have the opportunity to choose a ciphertext and get the plaintext for it (without knowing the key). What would you choose for the ciphertext?



Substitution Cipher

- In this cipher, each letter/character in the plaintext alphabet is substituted by a different letter/character in the ciphertext alphabet.
- If the alphabet we are using for the plaintext and ciphertext are both letters in the English alphabet, then the substitution cipher substitutes each letter for a different letter. In this case, the key is a **reordering** of the letters in the alphabet.
- For example, the key

ZYXWVUTSRQPONMLKJIHGFEDCBA

would mean A is mapped to Z, B is mapped to Y, etc.



Hands-on: Encrypt/Decrypt the Cipher

Encrypt the message “Never say never”
if the key is

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
R	Z	B	U	Q	K	F	C	P	Y	E	V	L	S	N	G	W	O	X	D	J	I	A	H	T	M

Note that the plaintext letters are provided in lowercase for convenience in this key.

Decrypt the ciphertext below, assuming it was encrypted with the key above:

RSRGGVQRURTEQQGXDCQUNBDNORART



Hands-on: Create Your Own Ciphertext

- Choose a key

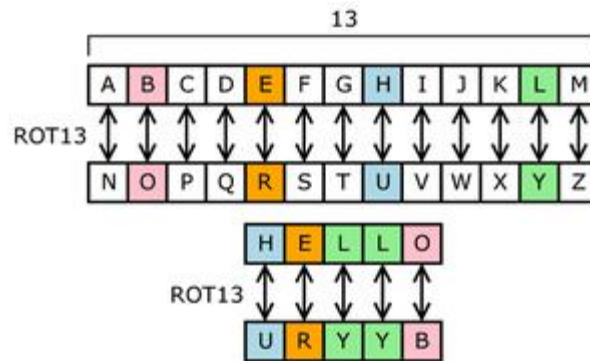
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

- Write your message
- Encrypt your message with the key, and write the ciphertext on a separate piece of paper.
- Provide the ciphertext to your neighbor
- What does your neighbor need to decrypt the message?
- Share what he/she needs with your neighbor.
- Decrypt the ciphertext that you get from your neighbor.



A Special Substitution Cipher: ROT 13

- Substitute each letter with another one according to the mapping in the diagram.



“[ROT13 table with example](#)” By Benjamin D. Esham ([bdesham](#)) derived from “[ROT13.png](#)” by [Matt Crypto](#). Public Domain.

- What is special about this cipher?
 - Encrypt a message using ROT13.
 - Then encrypt the resulting ciphertext again with ROT13.
 - What do you get?



Breaking the Substitution Cipher: Brute Force

- What is the key space? How many keys are there?
- How many permutations are there of the letters in English alphabet?
- Consider that there are 26 choices for mapping A, then 25 choices for B, 24 for C , etc. Using the multiplication principle we get

$$26 \times 25 \times 24 \times \dots \times 1 = 26!$$

which is a number of order 10^{26} which is $\sim 2^{88}$

- A huge number for brute force!



Substitution Cipher and Attack Scenarios

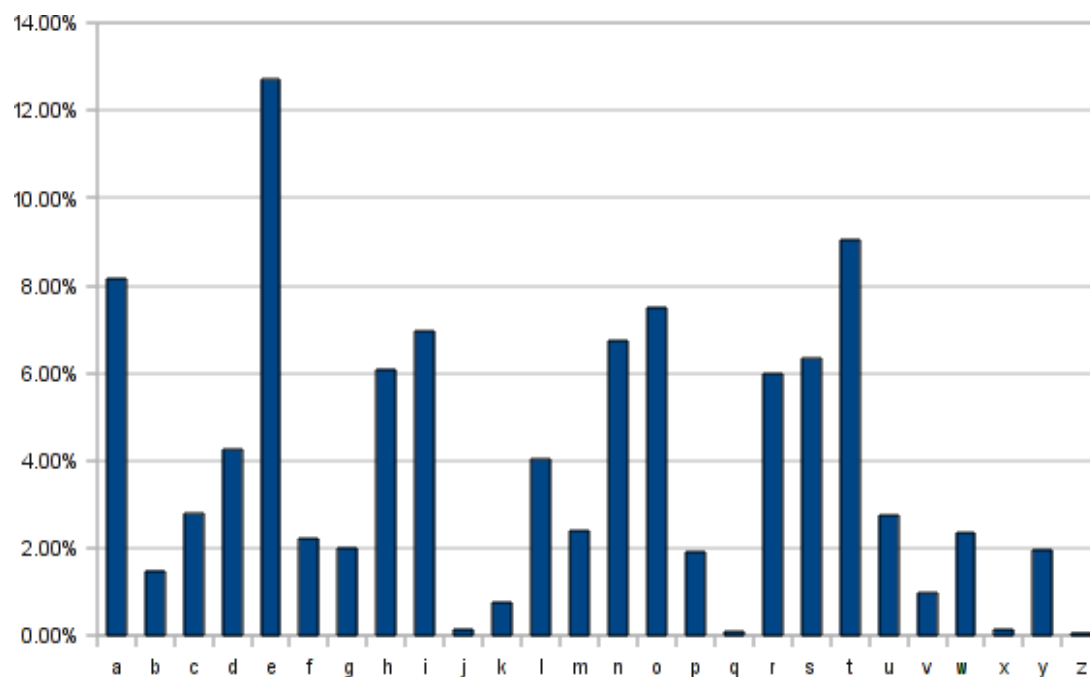
Task: Think about what it takes to decrypt a ciphertext that is obtained using the substitution cipher under these scenarios:

- **Ciphertext only attacks** – How can you proceed to break the cipher if all you have is the ciphertext ?
- **Known plaintext attacks** – You know that HELLO encrypts to MYZZK. Can you find the key? How can you proceed to find the key?
- **Chosen plaintext attacks** – You have the opportunity to choose a plaintext and get its ciphertext (without knowing the key). What would you choose for the plaintext?
- **Chosen ciphertext attacks** – You have the same ability as with chosen plaintext attacks, plus you have the opportunity to choose a ciphertext and get the plaintext for it (without knowing the key). What would you choose for the ciphertext?



Breaking the Substitution Cipher: Frequency Analysis

- In a long enough English text, the letters are distributed approximately as shown in this graph:



[“English letter frequency \(alphabetic\)”](#) by [Nandhp](#). Public Domain.



Breaking the Substitution Cipher: Frequency Analysis (continued)

- In addition to distribution of single letters, one can look at the distribution of pairs of letters (digrams) or triplets (trigrams) and substitute according to frequencies.



Frequency Analysis May Not Always Work

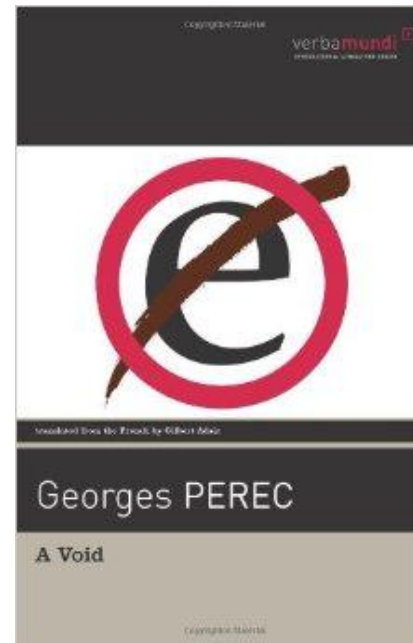
Copyrighted Material

racist attacks, with pogroms forming in such outlying Parisian suburbs as Drancy, Livry-Gargan, Saint-Paul, Villacoublay and Clignancourt. And stray acts of brutality abound: an anonymous tramp has his brains blown out just for a bit of moronic fun, and a sacristan is callously spat upon – in public, too – whilst giving absolution to a CRS man cut in half by a blow from a yataghan (a Hungarian slicing tool, if you must know).

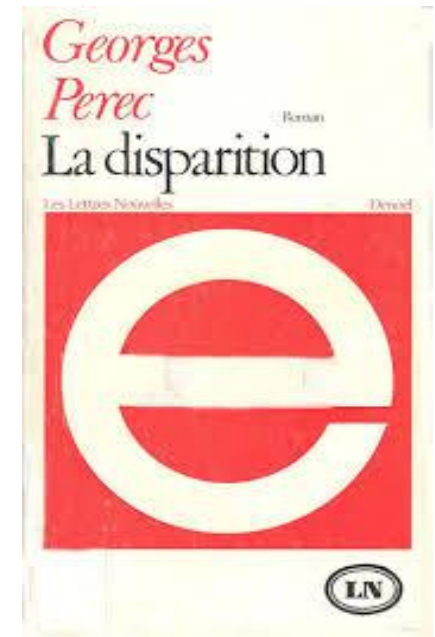
You'd kill your own kith and kin for a chunk of salami, your cousin for a crust, your crony for a crouton and just about anybody at all for a crumb.

On 6 April, from Saturday night until Sunday morning, 25 Molotov cocktails go off around town. Pilots bomb Orly airport. Paris's most familiar landmarks burn down, and its inhabitants look on in horror at a still blazing Alhambra, an *Institut* that is nothing but a sad, smoking ruin, a Saint-Louis Hospital with all its windows alight and gaily flaming away. From Montsouris to Nation not a wall is intact.

Opposition MPs add insult to injury by baiting a now almost suicidal ruling party, which, though obviously hurt by such an affront to its dignity, has a fair stab at smoothing things out. But whilst assassins start liquidating a handful of junior Quai d'Orsay officials (23, or so it's said), a Dutch diplomat caught filching an anchovy from a tub of fish is soon put paid to by an impromptu stoning. And whilst an odiously smug and arrogant viscount in shocking pink spats (*sic*) is laid into by Wagram's hoi polloi until his skin is of a similarly shocking colour (his only fault, it turns



©David R. Godine, Publisher.



©Denoël, publisher.



This document is licensed with a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/) ©2017 www.C5colleges.org

Modern Symmetric Ciphers

- There are several symmetric ciphers that are in use today. For example, the secure network protocol TLS/SSL (Transport layer Security/Secure Socket Layer) lists the following block ciphers in its suite of ciphers:

[RC4, Triple DES, AES, IDEA, DES, or Camellia](https://en.wikipedia.org/wiki/Cipher_suite)
(https://en.wikipedia.org/wiki/Cipher_suite)



NIST and Selection of Ciphers for Federal Processing

- National Institute of Standards and Technology (NIST)
 - Publishes guidelines for federal agencies to ensure that sensitive federal information is protected.
 - In 1973 the agency, then called the National Bureau of Standards (NBS), solicited algorithms to be used for protecting sensitive federal data.
 - In 1976 DES (Data Encryption Standard) was approved as a federal standard.
 - In 1997 NIST called for new algorithms to replace DES, as the key length (56 bits) used in DES was small for the increasing computational power.
 - In 2000 AES (Advanced Encryption Standard) was approved.



More on Modern Symmetric Ciphers

- DES – Data Encryption Standard (1977)
 - Algorithm used: Based on LUCIFER by IBM. Key size: 56 bits.
- 3DES – Triple DES (1999 – NIST approved)
 - Algorithm used: Triple application of DES. Key size: 112 bits.
- AES – Advanced Encryption Standard (2000)
 - Algorithm: Rijndael. Key sizes: 128, 192, and 256 bits.
- Other Finalists in the NIST search:
 - Serpent
 - Twofish
 - RC6
 - MARS



DES

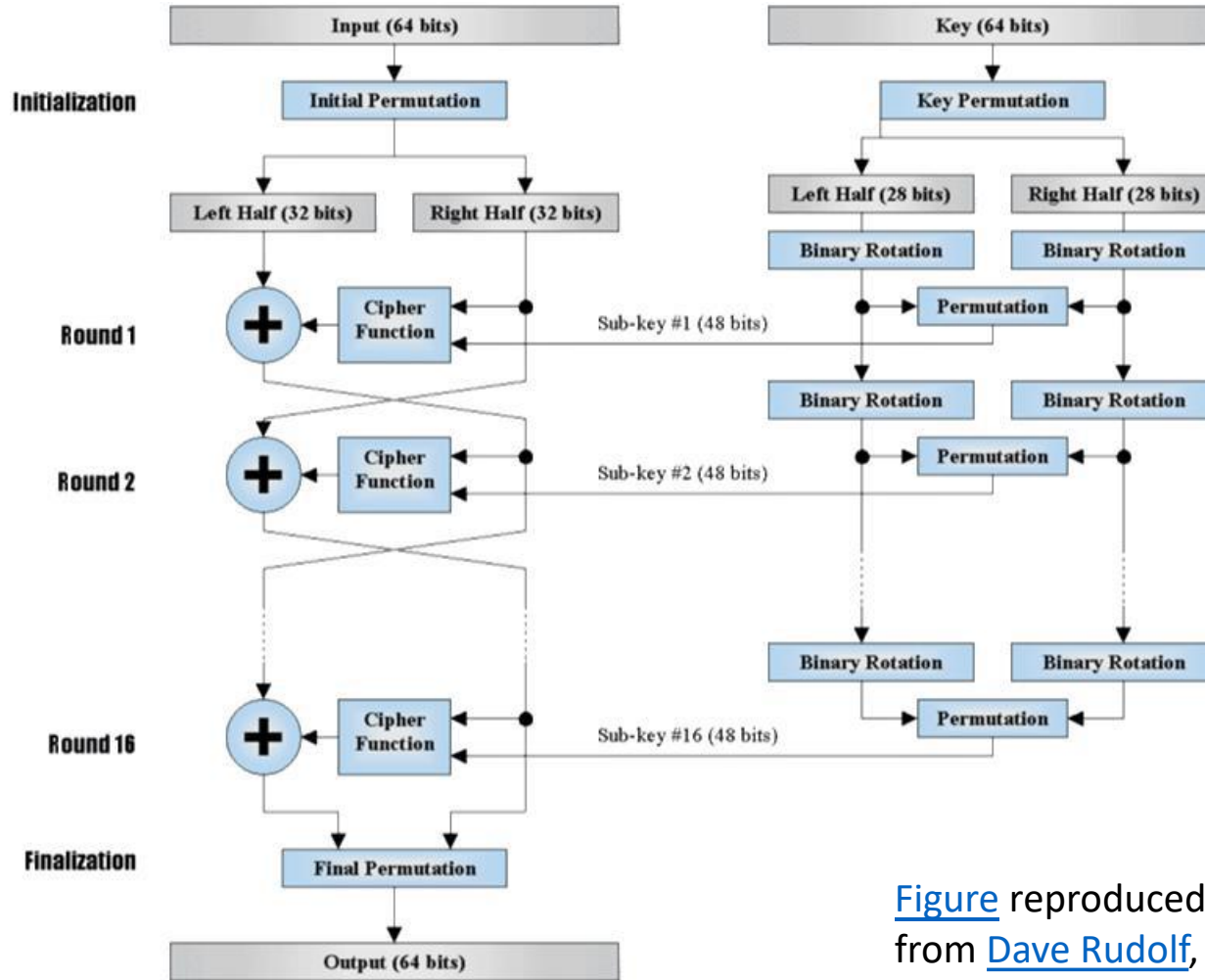
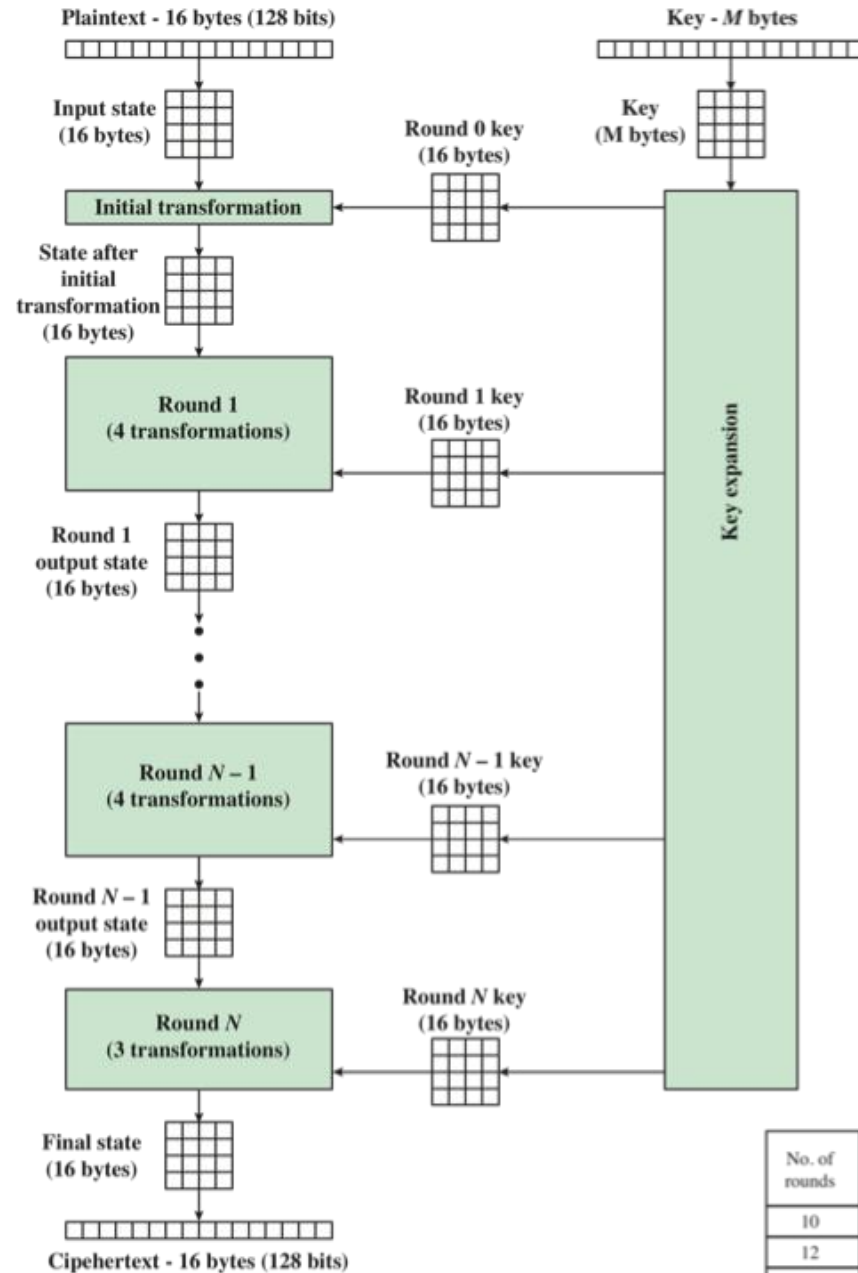


Figure reproduced with permission from Dave Rudolf, University of Saskatoon.

AES Encryption Process



“Figure 5.1: AES Encryption Process” *Cryptography and Network Security: Principles and Practice*. Stallings, W. ©2013 Pearson. Reprinted with permission from author.



Problem of Key Distribution and Management

- Modern symmetric key algorithms are great! They are fast and secure when implemented correctly and keys are chosen properly.
- Problem: How to get the keys to the two parties?
 - Need a secure channel – a channel that makes it very difficult for the adversary to access the actual plaintext that is being transmitted.
 - But the Internet is not secure!



Hands-on: Symmetric Encryption with Kryptos

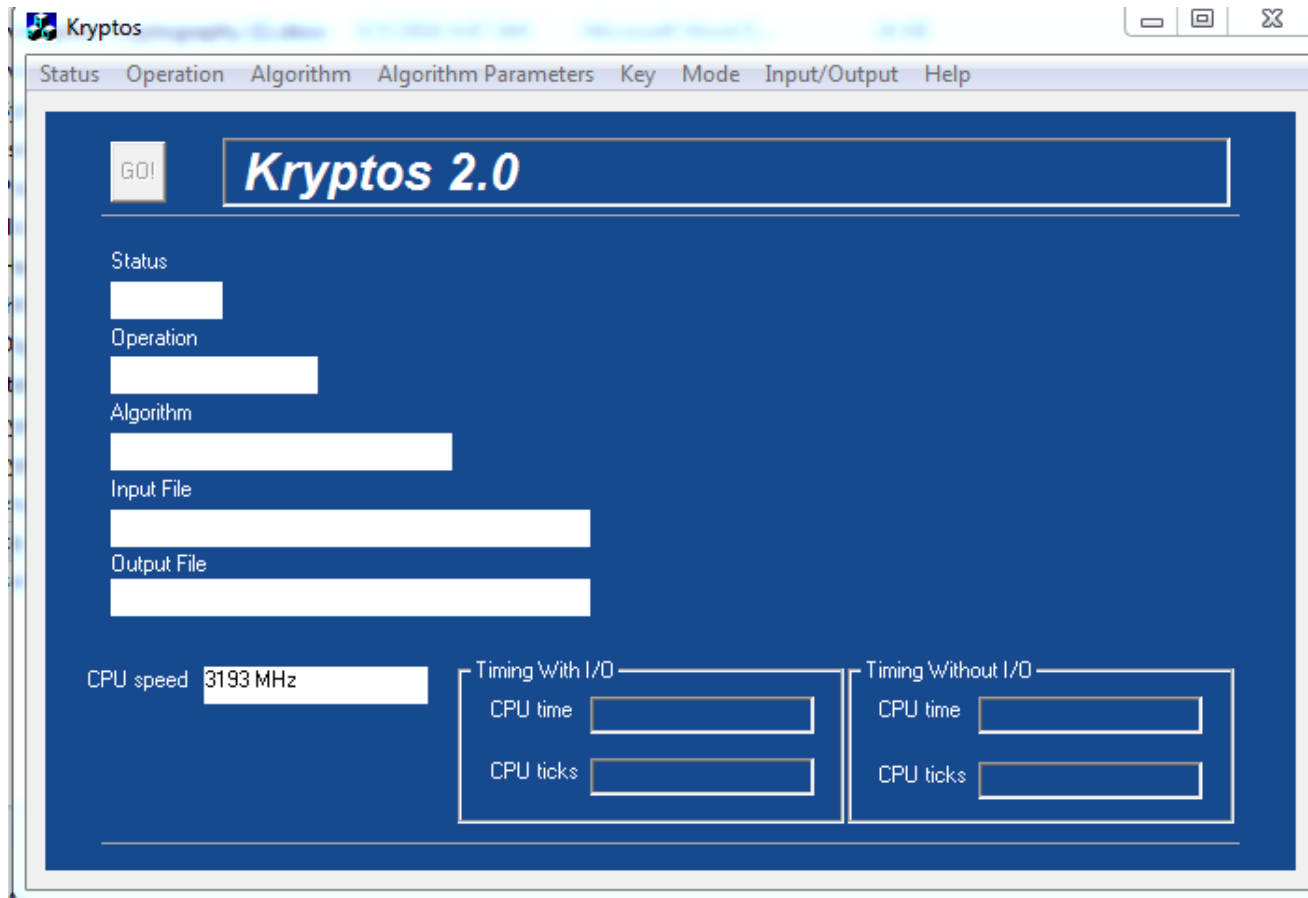
- Pair up with a classmate. You will be sending (via email) confidential messages to each other.
- In a text file, write a message to your partner. Save it in a folder that you can locate easily.
- Download Kryptos at

<http://sourceforge.net/projects/kryptosproject/files/Kryptos/Kryptos%202.0/>

DO NOT download the latest version (version 3.0) but version 2.0 (Kryptos.exe). The latest version may not work on your system.



Kryptos Software

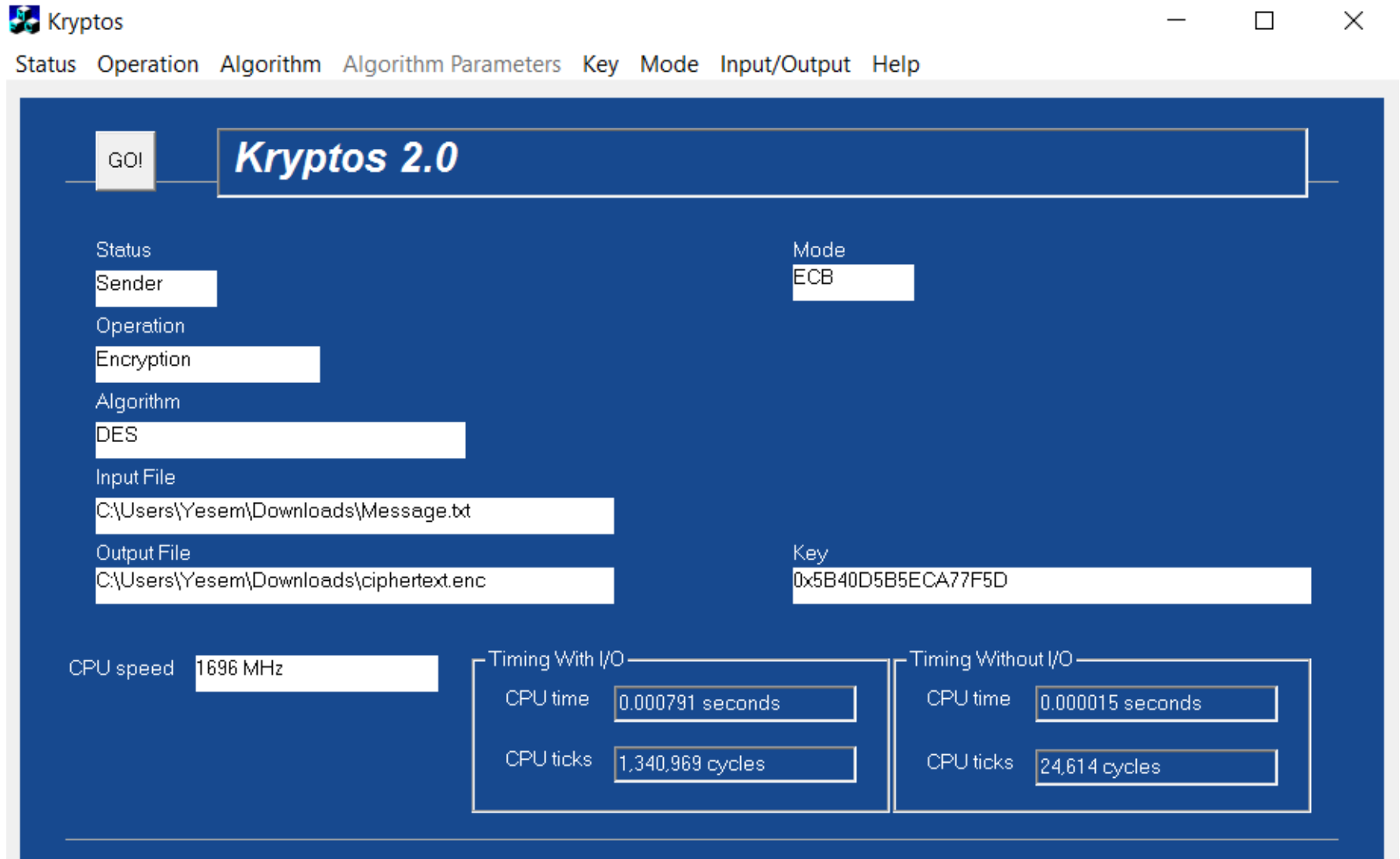


Encrypt Using Kryptos

- Follow these steps. (Use the Tab key to move from one field to the next.)
 - Status → Sender
 - Operation → Encrypt
 - Algorithm → DES
 - Key → Set Key → Select a Random Key → Generate Key → Save Key
 - Mode: ECB (Electronic Code Book)
 - Input /Output
 - Input → Create a message. (Choose the text file that you have created earlier.)
 - Output → Save the output to a file. (Use the default name or name it yourself.)
 - Hit GO!



Hands-on: Screen After Settings Completed — Hit GO!



The screenshot shows the Kryptos 2.0 application window. The title bar includes the application icon and name, and standard window controls. The menu bar contains: Status, Operation, Algorithm, Algorithm Parameters, Key, Mode, Input/Output, and Help. The main interface has a dark blue background with white text and input fields. A prominent 'GO!' button is located in the top left. The title 'Kryptos 2.0' is displayed in a large, stylized font. Below the title, there are several settings sections: 'Status' with a 'Sender' field, 'Operation' with an 'Encryption' field, 'Algorithm' with a 'DES' field, 'Input File' with a path 'C:\Users\Yesem\Downloads\Message.txt', 'Output File' with a path 'C:\Users\Yesem\Downloads\ciphertext.enc', 'Mode' with an 'ECB' field, and 'Key' with a hexadecimal string '0x5B40D5B5ECA77F5D'. At the bottom, there are performance metrics: 'CPU speed' at '1696 MHz', and two timing sections. 'Timing With I/O' shows 'CPU time' as '0.000791 seconds' and 'CPU ticks' as '1,340,969 cycles'. 'Timing Without I/O' shows 'CPU time' as '0.000015 seconds' and 'CPU ticks' as '24,614 cycles'.

Kryptos

Status Operation Algorithm Algorithm Parameters Key Mode Input/Output Help

GO! **Kryptos 2.0**

Status
Sender

Operation
Encryption

Algorithm
DES

Input File
C:\Users\Yesem\Downloads\Message.txt

Output File
C:\Users\Yesem\Downloads\ciphertext.enc

Mode
ECB

Key
0x5B40D5B5ECA77F5D

CPU speed 1696 MHz

Timing With I/O

CPU time 0.000791 seconds

CPU ticks 1,340,969 cycles

Timing Without I/O

CPU time 0.000015 seconds

CPU ticks 24,614 cycles

Hands-on: Share and Decrypt

- Send your ciphertext via email to your partner.
- What else do you need to send so that your partner can read your message?
- Upon receiving a ciphertext and other necessary information from your partner, decrypt the message. What does it say?
- What steps did you take to decrypt?
- Experiment with other ciphers/settings in Kryptos.





Catalyzing Computing and Cybersecurity in Community Colleges

is funded by a National Science Foundation grant and
is located at Whatcom Community College

237 West Kellogg Road
Bellingham, WA 98226

www.C5colleges.org

