



Title: Principles of Encryption

Subject: Science

Grades: 9 – 12

Category: Communications

Lesson Overview:

We hear a lot about privacy and security, especially for our lives online. Yet we rarely hear about how the need for privacy and security is met. As more of our personal lives end up on remote servers and in the hands of third parties, we will need to better understand how that data is protected. The basis of data protection is encryption: converting information from an easily understood form into a code that cannot be easily read or broken. In this activity, students develop and then compare and contrast three coding technologies based on principles of encryption. First, the students will construct a simple early cipher device, the Greek *scytale*. Second, the students will create a substitution code. Third, the students create a book cipher. Students will attempt to break the substitution code based on frequency analysis.

Learning Objectives:

Students will be able to:

- Explain the principle of encryption
- Use different methods to construct simple ciphers
- Understand the analytical principle behind breaking codes

Academic Standards:

National Science Education Standards (SCES)

Science as Inquiry: CONTENT STANDARD A

- Abilities Necessary to Do Scientific Inquiry
 1. Design and conduct a scientific investigation
 2. Use appropriate tools and techniques to gather, analyze, and interpret data.
 3. Develop description, explanation, prediction, and models using evidence.

Science and Technology: CONTENT STANDARD E

- Understandings about science and technology

Science in Personal and Social Perspectives: CONTENT STANDARD F

- Science and technology in local, national, and global challenges

History and Nature of Science: CONTENT STANDARD G

- Historical perspectives

Time Frame:

This lesson requires three 45-minute sessions to complete. The first session engages students and introduces the activity, during which students will construct a simple early cipher device, the Greek *scytale*. During the second session, the students will create a substitution code and a book cipher. During the third session, students will investigate frequency analysis as a method for breaking the substitution code.

Background for the Teacher:

In April 2011, hackers stole personal data of millions of online gamers from Sony, the makers of the Playstation gaming device. Why did a company as well known and resourced as Sony fall victim to such a large-scale hacking attack? Pundits and experts will undoubtedly debate that question for years to come. But the root of the problem was that Sony's security systems failed to stop the hackers breaking into the company's secure databases. This is a recent high profile example. But governments and law enforcement are continually engaged in cryptography, which has a history back into antiquity. Cryptography uses a combination of science, mathematics and linguistics. As more information moves online, a grasp of the elements of cryptography will be increasingly useful for our personal and professional lives. In this lesson, students will explore the basis of online security systems – encryption. Encryption is vital for secure computer transactions in our modern technology. When data is sent across a secure network, it is encrypted by sophisticated algorithms. These are based on encoding data. Understanding encryption will help students contextualize methods for encoding and decoding data. They will learn the basic principles that protect online data and provide privacy and security.

Vocabulary*

Book cipher - System of encryption that relies on using a passage in a book or other sources to substitute plaintext letters with letters.

Ciphertext – Text that has been encoded by encryption

Code breaker – Person (or program) that discovers a key or otherwise decodes a cipher

Cryptography – Methods or systems to encode messages or information

Cryptanalysis – Methods used to decode a message without the key

Decipher – To decode a message, with or without a key

Decode – to translate a message from code back into plaintext

Encryption – Process of encrypting or encoding a message

Key – Device or system that decodes a coded message

Plaintext – Text or message that is not encoded

Scytale – an early encryption device based

Substitution code – System of encryption that relies on substituting plaintext letters with letters or numbers according to a set of rules.

*First occurrences of vocabulary items are highlighted in the text.

Classroom Activities:

SESSION 1

Materials for the teacher:

- Model **scytale** prepared ahead of time* (optional)
- Photo or image of a scytale

*See instructions in Explore section



Image source: <<http://en.wikipedia.org/wiki/File:Skytale.png>>

Materials for each group of students:

- Paper
- Scissors
- Smaller diameter pen or pencil with hexagonal sides
- Larger diameter pen or pencil with round sides (such as a marker pen)
- Pen or pencil to write with
- Tape

Engage

1. Ask students if they have ever wanted to keep something secret. Ask students why they use passwords to access online accounts that include personal information, such as social networks.
2. Explain that passwords help secure data. But what happens to data when it is transferred? Explain the principle of **encryption** – taking information and encoding it so that the data is transformed. **Cryptography** is the science of methods or systems used to encode messages or information. The transformed data can only be understood with a key. The **key** literally unlocks the data to make it understandable to the intended recipient, but to no one else.
3. Explain that knowledge (or data) is access to power. Therefore the restriction of knowledge has been important throughout history. What if Al Qaida had access to information that the US Navy Seals were going to attack Osama Bin Laden's compound in Pakistan? What if Napoleon had known of

Wellington's troop deployment at Waterloo? What if the Persians had known the strength of the Greek forces at Thermopylae?

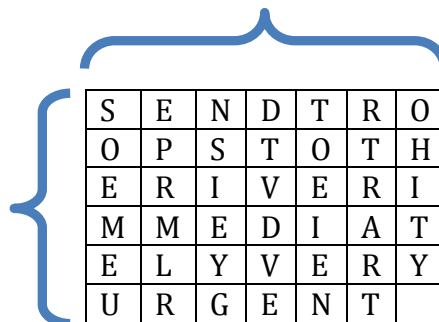
Businesses are also anxious to protect their own research, such as new technology that may give them a competitive advantage. In another example, earnings reports can dramatically affect share prices, so companies may want to keep financial information confidential. We trust that our day-to-day financial transactions such as shopping online or banking at an ATM are safe so that our account information is not exposed to unauthorized people. Although not all these examples involve encryption, history would be different if information had fallen into unwanted hands. Emphasize that military forces, law enforcement, businesses and governments have always needed to maintain secrecy for certain operations. The way to keep information secret is to encode it.

Explore

1. Present the materials to describe to students the scytale (pronounced "skih-tah-lee"), an early encryption device used by the Greeks. According to scholars, the ancient Greeks, and the Spartans in particular, used this cipher method to communicate during military campaigns. The students will create their own scytale. Have one group of students prepare the message. (See video demo to learn the basic principle of how it works.)
<<http://www.youtube.com/watch?v=GEICKI98EP8>>
2. The students use the scissors to cut a strip of paper half an inch wide. Tape one end of the paper to one side of the hexagonally sided pen. Carefully wind the paper around the pen, ensuring the wrapped paper does not overlap. Tape the other end. (The tape holds the paper to make writing on it easier.) This is the scytale. The hexagonally sided pen will allow the student to write eight to ten letters down each side (depending on the length of the pen). To encrypt the message, have students writes across the length of the pen a short message such as "SEND TROOPS TO THE RIVER IMMEDIATELY VERY URGENT." Explain that this is a **plaintext** message, which uses the everyday alphabet. Have them write in block capitals. Omit spaces between words and punctuation.

Eight columns correspond to number of times paper is wound around pen

Six rows correspond to hexagonal sides of pen



S	E	N	D	T	R	O	
O	P	S	T	O	T	H	
E	R	I	V	E	R	I	
M	M	E	D	I	A	T	
E	L	Y	V	E	R	Y	
U	R	G	E	N	T		

3. Remove the tape and unwind the strip of paper.
4. When the strip is unwound, the strip of paper will have the encrypted text in the order of letters around the sides:
“SOEMEUEPRMLRNSIEYGDTVETOWIENRTRARTOHYTY”
5. Divide the remaining students into two groups, “enemy” and “friend.” Their job is to decipher the message. Give the “enemy” group the round pen and give the “friend” group a hexagonally sided pen.
6. Introduce the concept of the key. The key unlocks the code. In this case, the key is the correct sized pen.

Explain

1. Explain that text that has been encoded is called **ciphertext**. Explain that to **decipher** a message is to **decode** it, with or without a key
2. Explain that to decipher the message, the students must wrap the strip of paper around the correct size of pen. The “enemy” group using the large round pen will get a garbled message. The “friend” group will be able to decipher the message.
3. Ask students why one size of pen correctly deciphered the message and the other did not.

Extend

1. Explain to students that Greeks did not have modern pens, so they used carved wooden rods.
2. Explain the scytale is an example of a transposition cipher, in which letters are shifted according to specific rules, in this case determined by the device.
3. Have the students discuss the advantages and disadvantages of this method of encryption. It is easy to use but also easy to decipher if the “enemy” has the correct diameter of rod. The method is suitable only for short messages.
4. Discuss other methods of encryption and the risks and benefits of using various alternatives.
5. Explain that all methods of encryption are vulnerable to decryption.

Evaluate

1. What is one advantage and one disadvantage of the scytale as a method of encryption.
2. How could the scytale be modified to hinder decryption?
3. Are there better ways to encrypt information than using transposition encryption?

Scoring key for evaluation

1. One advantage is that it is quick and easy to use for both encrypting a message and deciphering it. A disadvantage is that an enemy can easily decipher the message if they have the correct sized rod.
2. The scytale could be modified so that you needed a special kind of rod instead of a widely available pen. For example, if the rod diameter varied, so that it was one inch at the beginning and two inches at the end, decryption would be difficult without that exact same rod.
3. Another way to encode information might be to systematically substitute one letter for a different one.

SESSION 2

Materials for the teacher:

- Timer

Materials for each group of students:

- Pencil or pen
- Paper
- Literary book

Engage

1. Following from Lesson 1, ask students how they might create a code that is hard to break.
2. Describe the need for secrecy in military operations. For example, the Germans used a coding machine called Enigma. During World War Two, the Enigma machine enabled Germans to attack Allied shipping. However, when the machine was captured on a German U-boat, the Allies were able to decode intercepted German messages. The intercepted messages enabled the Allies to find and destroy German U-boats, turning the tide of the war.

Explore

1. Present the materials to students. Explain that with these simple tools they can create codes that are hard to break.
2. Ensure students understand that there are many ways to create codes. They will use two simple ways to create their own complex codes. Explain that even they can vary these simple methods to create endless variations of a code.

Explain

1. Explain that two simple methods of encryption have been widely used, the **substitution code** and the **book cipher**. Students will create examples of both.

2. Explain the principle of the substitution code. The simplest example is to shift letters of the alphabet so that one letter is consistently substituted for another. For example, a downshift of one letter makes A=B, B=C, C= D and so on. Therefore, “SEND TROOPS TO THE RIVER” becomes “TFOE USPPST UP UIF SJWFS.” Letters can be upshifted (A=Z, B=Y, C=X, etc.) or shifted by more than one letter (e.g., A=C, B=D, C=F, etc.).
3. Explain the principle of the book cipher. The book cipher is a variation of the substitution code, except that a page in a book or other text is used as the basis of substitution. Explain that book ciphers became popular only with the proliferation of printed books. In the book cipher, the coder skips repeated letters and spaces until most or all of the letters of the alphabet are keyed. For example, using the first sentence of the Declaration of Independence:

“We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights”

The passage only has fifteen unique letters, as highlighted below:

We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights”

Therefore the key for the first fifteen unique letters of the alphabet is:

WEHOLDTSRUBFVINAMCQY= ABCDEFGHIJKLMNOPQRST

For letters not included in the key (i.e., that don’t appear in the selected book cipher sentences), simply continue from the last letter in the sequence, so for the above code, the 26 letters of the alphabet are

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

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

So “SEND TROOPS” becomes “QLIO YCNNAQ” and so on.

Extend

1. Divide students into three groups. One group is the code makers, another group is the code decipherers. The third group is the **code breakers**.
2. Have code maker group create their own substitution codes or book ciphers and then create messages based on their codes. Have the students use their own choice of book for the book cipher.
3. The code maker group passes on their coded messages to the decipherer group and to the code breaker group. The latter groups decode, or attempt to decode the messages. The decipherer group receives the key (rules for the substitution code or the key to the book cipher), while the code breakers do not.
4. Time students for how long the groups take to decode the messages. The group with the key should be able to decipher the message within a few

minutes. The group without the key will be most likely be unable to break the code in the allotted time.

Evaluate

1. Discuss the merits of the two methods of encryption. Which is more practical and why?
2. Which code would be easier to break and why?
3. Is it possible to break the book cipher without knowing the key?

Scoring key for evaluation

1. The substitution cipher is relatively easy to use, and layers of variation can be built in, such as double substitution. The book cipher requires that the person deciphering the message has the correct book. Both methods can take a long time to encode and decode a message.
2. The book cipher is much harder to break than the substitution cipher, because it does not rely on a consistent rule to encode information.
3. If an adversary obtains the book they can easily get the key and break the code. Otherwise, a book cipher can be very difficult to break unless we use statistical techniques.

SESSION 3

Materials for the teacher:

- Table of letter frequencies
- Histogram of letter frequencies

Materials for each group of students:

- Pencil or pen
- Paper
- Computer with spreadsheet application (optional)

Engage

1. Students have learned the basics of encryption. But why would it be desirable to decrypt a message, to break a code? If Al Qaida was using coded information to plan attacks on the United States, we would want to break their code in order to protect the safety of the American people. If drug cartels were using codes to plan smuggling operations, we would want to break their codes in order to stop illegal drug trade.
2. How are codes broken?
3. Explain that cryptographers have worked throughout the ages to find the perfect code. Ideally a code is readily deciphered by the intended recipient but unbreakable without a key. In practice, creating an ideal code is very difficult. One reason is that our language follows certain rules. If we apply

such rules to coded information, we can usually break a code, although that might take a lot of work.

4. The advent of cheap computing power has made encryption and decryption much faster than previously possible.

Explore

1. How do cryptographers decode messages when they do not have the key? Explain that **cryptanalysis** is used to decode a message without the key.
2. Cryptanalysis uses a statistical approach to discovering patterns and rules in encoded messages. Such patterns and rules can then be correlated to known patterns and rules in language.
3. Why is cryptanalysis important? If an enemy is sending an encoded message, it needs to be decoded, but that would need the key. Cryptanalysis can help recreate the key to decode enemy messages.

Explain

1. Explain that one of the simplest methods for code breaking is frequency analysis. This method relies on the fact that some letters occur more frequently in language than others. Samuel Morse, who created the Morse Code (a kind of simple binary messaging system) used letter frequency to develop his system. Anyone who has played Scrabble knows that some letters score more highly than others. For example, Z and Q score 10 in Scrabble, while J and X score 8. All the vowels and some other letters score only 1. From these scores, we can infer high scoring letters occur less frequently than others.
2. Present students the table of letter frequencies. Show students the histogram of letter frequencies. Compare these with letter scores in Scrabble.
3. Explain that these frequencies can be used to decipher text messages without a key.
4. Have students create a message with the substitution code or book ciphers they used in the previous lesson. Have them create a message that includes of about 100 letters.
5. Have the students take the coded message and rank the letters according to the number of times they occur in the message frequency. For example, the ranked letter frequency for "TFOE USPPST UP UIF SJWFS" would be as follows:

S = 4

U = 3

P = 3

F = 3

T = 2

O = 1

E = 1

I = 1

J = 1

W = 1

6. Have students create two columns in the spreadsheet, one for letters and the other for the corresponding frequency. As a check, ensure the sum of the ranked letters equals the total number of letters in the message (=20 in the above example).
7. At this point, introduce the concept of probability. If the message is long enough, the frequencies of letters in the message will converge on the frequencies in the table. Therefore, there is a high probability that the coded S is the most frequent letter. Therefore, one can hypothesize that S is E. The hypothesis is then tested by substituting back the letters to see if any of the words make sense. For example, if encoded S = plaintext E, the message becomes: "TFOE UEPPET UP UIF **EJWFE**" which still doesn't make sense. Next one could hypothesize that the coded U is E, and so on. Using this method, hypothesized letters are continuously refined until a meaningful message emerges. For example, since A and T are the two commonest letters in words, one can hypothesize that encoded F = plaintext E, and U = T, the message becomes: "TEOE TSPPST TP **TIE** SJWES." This doesn't seem helpful but knowledge of English can help. Take the third word. If 'ie' does begin with T, how many two lettered words in English begin with T? There is only one common example, "TO." Therefore, let's hypothesize that encoded P = plaintext O. Substitute again, and the message now becomes "TEOE **TSOOST** TO TIE SJWES." Try the same thinking with the fourth word. What three letter words begin with T and end in H? "THE" is the only commonly used word, so hypothesize that encoded I = plaintext H. The message is now: "TEOE **TSOOST TO THE** SJWES." Frequency analysis allows quick testing of other combinations.
8. The above example demonstrates that a large sample size (message length) increases the speed of successful deciphering. There is too little information in a short message to readily correlate the frequency of letters in the message with those in the table. Frequency analysis requires testing of many letters before getting a meaningful message.

Extend

1. Frequency analysis is a simple but powerful way to break a code. Many cipher systems are vulnerable to frequency analysis. Discuss ways that would make it harder to break a code, such as double encoding or numeric substitution
2. Have students brainstorm to think of other methods of encryption including:
 - a. Transposition ciphers – like the scytale, these transpose letters by means of a device or algorithm.
 - b. Steganography – Hides a message within another message, such as using the first letters in each word of a sentence, or some other rule. A template uses a pattern to highlight certain words in a coded message.
3. Introduce students to the basics of public key cryptography, which uses two keys. The public key is known by everyone who needs to send a message. The private key is known only to the recipient. For example, everyone knows your email address, but a password is needed to "unlock" the email message.

4. Ask students for examples where encryption is necessary and where it fails. For example, the human factor plays a role. If someone betrays the key to the enemy, the encryption method becomes obsolete. Governments and security organizations are therefore very protective of encryption keys.
5. Ask students why encryption is important. Relate it to online security, such as when they visit a website with the https protocol. What does that mean?
6. Given that so much of our information is online what are the countervailing pressures to encrypt and decrypt information? Explain this is similar to an arms race. Methods of encryption will continually improve and evolve, as will methods to decrypt information.
7. Discuss careers in cryptology and related fields.

Evaluate

1. Why is sample size (length of message) important in frequency analysis?
2. What is the likelihood that the following messages (a) and (b) are meaningful or just random collections of letters? Explain your reasoning.
 - a) XRXBJIPSGBHWMCJQRONKMISKCWUPXFFAZKLEEKTESVLNMHZEQDGT
FCZSPCQBVGKYPFQDOPRUJMAFHJOLXLMCQVJWOOVUIRLAYYTN
 - b) YSLQPXWHYQYCRBLQWEFWIHLLEYKLLIACLQLCJRITFLTRYRVWYLW
IOELIRTIGQLQNDYLHSINFNTXWIOACNYLHYRITKLHNIQGQLCQ

Scoring key for evaluation

1. Sample size (length of message) in frequency analysis is important because letters do not occur at a random frequency in written language. We can use non-random patterns to determine the key for a message. As sample size increases, frequency of letters in the encoded message converge upon those in written language. Hypotheses about the correct identity of letters can be tested, enabling the key to be determined.
2. The letter frequencies in message (a) range from 3 to 5, which is less variation than we might expect in written language. The letter frequencies in message (b) range from 1 to 16, which is consistent with the variation of letter frequency in the written language. Moreover (b) contains two sets of three repeated letters, “WIO” suggested a common three letter word. Most likely (a) is a random sequence of letters, and (b) contains meaning.

Teacher note:

Message (a) is a random set of 100 letters generated using an online tool:

<<http://www.dave-reed.com/Nifty/randSeq.html>>

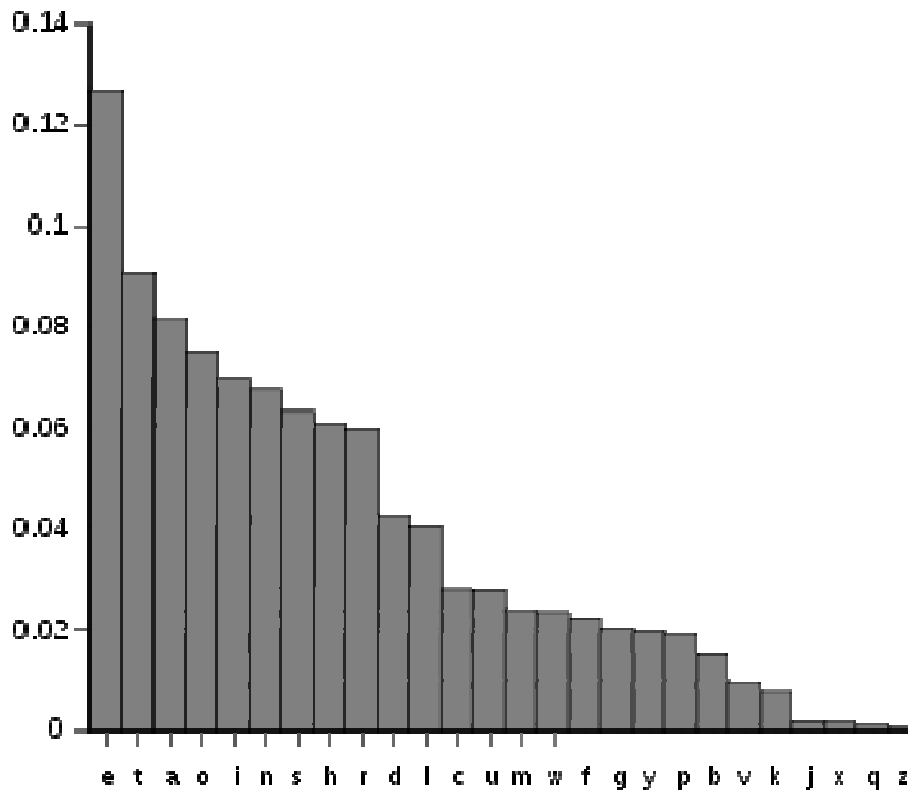
Message (b) is a paraphrase by Cliff Stearns, which is encoded using the book cipher in Session 2 using the Declaration of Independence key. The decoded message reads: “The Spy Act strikes a balance between preserving legitimate and benign uses of technology and protecting we consumers.” The repeated three letter word is “AND.”

TABLE OF LETTER FREQUENCIES

(Source: <http://en.wikipedia.org/wiki/Letter_frequency> based on references in Further Reading)

Letter	Frequency
a	8.167%
b	1.492%
c	2.782%
d	4.253%
e	12.702%
f	2.228%
g	2.015%
h	6.094%
i	6.966%
j	0.153%
k	0.772%
l	4.025%
m	2.406%
n	6.749%
o	7.507%
p	1.929%
q	0.095%
r	5.987%
s	6.327%
t	9.056%
u	2.758%
v	0.978%
w	2.360%
x	0.150%
y	1.974%
z	0.074%

Figure 1. Histogram of relative frequency of letters.





Web resources

How Encryption Works

<http://www.howstuffworks.com/encryption.htm>

Cryptography, Tom Linton, Central College

<http://pages.central.edu/emp/LintonT/classes/spring07/cryptoframeset.htm>

Video demo of how to create a scytale

<http://www.youtube.com/watch?v=GE1CkI98EP8>

Clear Focus on Risk Leads to Laptop Security by Malcom Harkins, Chief Information Security Officer, Intel Corporation

<http://www.indefenseofdata.com/2011/01/clear-focus-on-risk-leads-to-laptop-security>

CrypTool (free, open-source e-learning application)

<https://www.cryptool.org>

Hide a Message Inside an Image!

<http://mozaik.org/encrypt/> & <http://mozaik.org/decrypt/>

How has cryptography been used throughout the ages?

<http://curiosity.discovery.com/question/how-cryptography-used-throughout-ages>

How is encryption important to Internet communications?

<http://curiosity.discovery.com/question/encryption-important-internet-communications>

Why is symmetric-key encryption important?

<http://curiosity.discovery.com/question/why-symmetric-key-encryption-important>

How does public-key encryption ensure security?

<http://curiosity.discovery.com/question/public-key-encryption-ensure-security>

What is the importance of a hashing algorithm in encryption?

<http://curiosity.discovery.com/question/importance-hashing-algorithm-encryption>

Further reading

Beker H. & Piper, F. (1982) *Cipher Systems: The Protection of Communications*. Wiley-Interscience.

Lewand, R. (2000) *Cryptological Mathematics*. The Mathematical Association of America.

Trappe, W. & Washington, L. C. (2006) *Introduction to Cryptography with Coding Theory*. Pearson Education.

STUDENT TAKEAWAY – Principles of Encryption

Vocabulary

Book cipher - System of encryption that relies on using a passage in a book or other sources to substitute plaintext letters with letters.

Ciphertext – Text that has been encoded by encryption

Code breaker – Person (or program) that discovers a key or otherwise decodes a cipher

Cryptography – Methods or systems to encode messages or information

Cryptanalysis – Methods used to decode a message without the key

Decipher – To decode a message, with or without a key

Decode – to translate a message from code back into plaintext

Encryption – Process of encrypting or encoding a message

Key – Device or system that decodes a coded message

Plaintext – Text or message that is not encoded

Scytale – an early encryption device based

Substitution code – System of encryption that relies on substituting plaintext letters with letters or numbers according to a set of rules.

What is encryption?

Encryption is a systematic way of encoding information so that only the intended audience is capable of receiving a coded message. People have been encrypting messages since antiquity.

How are messages encrypted?

All encryption approaches involve transforming information in *plaintext* using a systematic method called a *cipher*. Only those with a *key* to the cipher can decode the message.

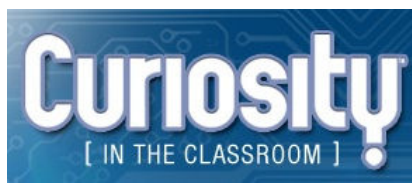
What are the main techniques of encryption?

Cryptologists recognize three primary techniques for encrypting messages.

1. Translation jumbles letters using a device that may also serve as the key.
2. Substitution replaces one letter with another according to one or more rules.
3. Steganography hides a message within another message.

How can codes be broken?

The most efficient way to break a code is by frequency analysis. Letters occur in language with non-random frequencies. Therefore a code breaker can detect patterns in coded information and make inferences about how letters in the code correspond to plaintext.



Who is concerned about encryption?

The military, governments, law enforcement and businesses encrypt information to protect it. Anyone who has information online should be concerned about whether their personal data is protected by encryption.

Why is encryption important?

Most of our personal information including school and medical records, and employment history is stored in online databases. Social networking profiles and online email includes information about our activities and contacts. If this information was available to anyone, it could be used for unwanted purposes such as targeted advertising. A worse scenario is that personal information could be used for undesirable purposes. Blackmailers and identity thieves find endlessly creative ways to use our personal information in ways that damage reputations, credit records, and relationships with prospective partners or employers.

Web resources

How Encryption Works

<http://www.howstuffworks.com/encryption.htm>

Cryptography, Tom Linton, Central College

<http://pages.central.edu/emp/LintonT/classes/spring07/cryptoframeset.htm>

Video demo of how to create a scytale

<http://www.youtube.com/watch?v=GE1CkI98EP8>

Clear Focus on Risk Leads to Laptop Security by Malcom Harkins, Chief Information Security Officer, Intel Corporation

<http://www.indefenseofdata.com/2011/01/clear-focus-on-risk-leads-to-laptop-security>

CrypTool (free, open-source e-learning application)

<https://www.cryptool.org>

Hide a Message Inside an Image!

<http://mozaiq.org/encrypt/>

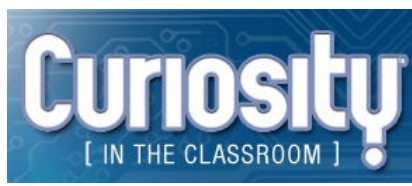
<http://mozaiq.org/decrypt/>

How has cryptography been used throughout the ages?

<http://curiosity.discovery.com/question/how-cryptography-used-throughout-ages>

How is encryption important to Internet communications?

<http://curiosity.discovery.com/question/encryption-important-internet-communications>



Sponsors of Tomorrow: 

Discovery
EDUCATION™

Why is symmetric-key encryption important?

<http://curiosity.discovery.com/question/why-symmetric-key-encryption-important>

How does public-key encryption ensure security?

<http://curiosity.discovery.com/question/public-key-encryption-ensure-security>

What is the importance of a hashing algorithm in encryption?

<http://curiosity.discovery.com/question/importance-hashing-algorithm-encryption>