|  |
| --- |
| Listening  Speaking  Reading  Grammar  Writing |
| **Topic:** Cryptography |

|  |  |  |  |
| --- | --- | --- | --- |
| **Instructor:**  Mega | **Level:**  Intermediate. | **Students:**  **#7** | **Length:**  30 Minutes |

|  |
| --- |
| **Materials:** - Computer (with internet connected) with beam project.  - Worksheets(Main activity) 6copies  - Hand-outs(help Ss to make a cryptogram, Text for Main activity) 6 copies  - Pictures(Picture of Scytale, Picture to explain encrypted and decrypted & Plaintext and Ciphertext, Picture to show Vigenère square, Picture to show Alphabets of Olivier Levasseur, Picture of the Enigma Machine) to explain key words |

|  |
| --- |
| **Aims:**  - Ss will be able to use and know cryptogram by post activity.  - Ss will be able to use prepositions with time by main activity.  - I want to be confident and encouraging in class and give clear instructions |

|  |
| --- |
| **Language Skills:**  Phonology: /i/ /e/ /f/ /p/ ex) vigenere cipher  Lexis: encrypt, decrypt, plain text, and cipher text  Grammar: preposition uses with time  Function: giving instructions, guessing the answers.  Discourse: Discussion, instruction |

|  |
| --- |
| **Language Systems:**  Listening: Ss will listen to the instructions from teacher.  Reading: Ss will read a text from main activity and instructions from post activity.  Writing: Ss will write answers on worksheet.  Speaking: Ss will share their experience and discuss with other Ss |

|  |
| --- |
| **Assumptions:**  - Ss should not have any trouble reading the main text.  - Ss should be able to do every activity with no problem. |

|  |
| --- |
| **Anticipated Errors and Solutions:**  - Multi-media might not work: Use board to explain  -Ss might be afraid to speak up: encourage them with comments like “good job!!”, “ you are doing great” and “ you are on right track” “go on” |

|  |
| --- |
| **References:**  <http://blog.simplilearn.com/it-security-management/understanding-cryptography> (Picture of Scytale)  <http://www.onlinebusiness.newstipstricks.com/what-is-cryptography/> (picture to explain encrypted and decrypted & Plain text and Cipher text)  <https://securityblog.redhat.com/2013/08/14/a-brief-history-of-cryptography/> (Text for Main activity)  <http://en.wikipedia.org/wiki/File:Enigma.jpg> (picture of Enigma machine)  <http://pifflelab.com/2012/05/27/microsoft-word-using-vba-to-encrypt-text-using-caesar-and-vigenere-ciphers/> (piture to show Vigenère square)  <http://libertalia.re/wp-content/uploads/2013/12/2.png> ( Picture of Alphabet of Olivier Levasseur)  <http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher> (Instructions for post activity) |

|  |  |  |
| --- | --- | --- |
| **Lead-In** | | |
| Materials: N/A | | |
| Time | Set Up | Procedure |
| 2  mins | Whole class | **[Opening Comments]**  - Hello, guys. How are you doing, today? Are you ready to learn something new? I have a question for you. Have you ever written a secret message to your friends? Or have you ever seen people using secret codes?  - Ss answer -> Yes or no and use their schemata to tell their experience |

|  |  |  |
| --- | --- | --- |
| **Pre-Activity** | | |
| Materials: - Realia (Pictures of vocabulary)  - Computer with beam projector | | |
| Time | Set Up | Procedure |
| 5 mins | Whole class | **TT:** Do you know what they are called? – Ss answer -> No -> It is called cryptography.  Show the topic : cryptography  **[Warm-up]**  Words and Examples.  **Show the first picture of ppt(power point) and elicit by making them guess first and then go on with the ppt to give hints. If it’s sure that they have understood the meaning than say “great!” or “awesome” or “you are doing great”**  **New vocabulary**  **-Cipher**  **-Plain text**  **-Cipher text**  **-Encrypting & Decrypting**  **-Scytale**  **-The Enigma machine**  **1. Plain text, Cipher text, encrypting, and decrypting:** Let Ss guess first (Teacher’s talk(TT): Here is a picture of Tom & Alice, What can you tell by just looking at it? Or what are Tom and Alice doing) -> Ss anwer by looking at the picture.  **CCQ:** When you encrypt some message, is the message readable?  **Ex)** Can you give me some sentences using these words by looking at the picture? -> Ss answer like Tom is encrypting the message or Alice has decrypted the message from Tom.  **2. Scytale:** Let Ss guess -> tell them who used it and how to use it.  **TT:** It is used by the ancient Greeks and the Spartans.  **CCQ:** Do you use scytale for hanging your clothes? – Ss answer: No |

|  |  |  |
| --- | --- | --- |
| **Main Activity** | | |
| Materials: -Computer with a beam projector  - Hand-outs for Main text. (6 copies)  - 6 copies of Vigenère square hand-out.  - | | |
| Time | Set Up | Procedure |
| 5 mins  7 mins |  | **[Elicit and showing exmaples]**  (Show some example words that are made of alphabets of Olivier Levasseur)  **Ex Words:** Mega, Tobin, Cryptography, You are awesome.  **TT:** Here, can you guess what these symbols mean? Or what they are? – Ss answer -> Yes or No  (Show the picture of Alphabets of Olivier Levasseur)  **TT:** Take a look at this. And can you tell me what the words stands for?  - Ss answer by giving the right meanings of the words.  **TT:** Use this table to make the words from the slide.  - Ss make the given words  **[Reading with scanning skill]**  **TT:** You are going to read something interesting. Don’t look at it yet.  You have to answer questions on next page. Ok? But We will do first 2 questions together. And the rest of it, you are going to answer with your partner.  **ICQ:** -How many Q’s (questions) are we going to answer together?  - Are you going to answer the other Q’s on your own?  **TT:** Good!!! Question 1:………………..? Now, I want you to scan for the answer!! I’ll give 20 sec to find it. Starting from….Now!!! Go!!!  Who got it?  - Ss answer and share their answers.  Do same with Q 2  (after answering first 2 Q’s)  - Now you have 3 mins to read and answer the Q’s  -Give time warning(1 min) |

|  |  |  |
| --- | --- | --- |
| **Post Activity** | | |
| Materials: Hand-out (Vigenere Square) 6 copies  Computer with beam projector | | |
| Time | Set Up | Procedure |
| 2 mins  5 mins |  | [Elicit]  **TT:** Were you able to understand the text? No? OK…It was just quick view on history of cryptography. Let’s move on, guys.  Who wants to try making cryptogram? I think you do~!!! And I think you are ready for it!!!!  [Instructions]  **TT:** This is how it is going to work. I will give you an example.    Plain text: ATTACKATDAWN  Key word: LEMONLEMONLE  Cipher text: LXFOPVEFRNHR  I want to make a message “ Attack at dawn into cipher text”  I chose Key word to be “LEMON”  So, I am going to use rows for my key word and columns for my plain text  I am on row ‘L’ and column ‘A’ and it ends up with letter ‘L’ and go on.  Let’s try making some words with it. Let’s start with your own name and make any sentence you feel like.  [Monitor Ss and help them if they are having trouble]  I will give 5 mins |

|  |  |  |
| --- | --- | --- |
| **S.O.S Activity** | | |
| Materials: N/A | | |
| Time | Set Up | Procedure |
|  |  | [ Have discussion briefly about what are some ways to make cryptogram useful] |

Attachments

**1.** Picture of Scytale

**2.** Picture to explain encrypted and decrypted & Plaintext and Ciphertext

**3.** Text for Main activity

**4.** Picture to show Vigenère square

**5.** Picture to show Alphabets of Olivier Levasseur

**6.** Picture of the Enigma Machine





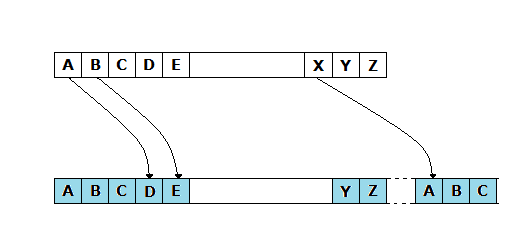
|  |
| --- |
| Name: .Date: . |

# A Brief History of Cryptography

Cryptology is a young science. Though it has been used for thousands of years to hide secret messages, systematic study of cryptology as a science (and perhaps an art) just started around one hundred years ago.

The first known evidence of the use of cryptography (in some form) was found in an inscription carved around 1900 BC, in the main chamber of the tomb of the nobleman Khnumhotep II, in Egypt. The purpose was not to hide the message but perhaps to change its form in a way which would make it appear dignified. Though the inscription was not a form of secret writing, but incorporated some sort of transformation of the original text, and is the oldest known text to do so. Evidence of some use of cryptography has been seen in most major early civilizations. “Arthashastra”, a classic work on statecraft written by Kautalya, describes the espionage service in India and mentions giving assignments to spies in “secret writing” – sounds like an ancient version of James Bond?

Fast forwarding to around 100 BC, Julius Caesar was known to use a form of encryption to convey secret messages to his army generals posted in the war front. This substitution cipher, known as Caesar cipher, is perhaps the most mentioned historic cipher in academic literature. In a substitution cipher, each character of the plain text is substituted by another character to form the cipher text. The variant used by Caesar was a shift by 3 ciphers. Each character was shifted by 3 places, so the character ‘A’ was replaced by ‘D’, ‘B’ was replaced by ‘E’, and so on. The characters would wrap around at the end, so ‘X’ would be replaced by ‘A’.

[](https://rhsecurity-sparks.rhcloud.com/wp-content/uploads/2013/07/caeser-cipher.png)

It is easy to see that such ciphers depend on the secrecy of the system and not on the encryption key. Once the system is known, these encrypted messages can easily be decrypted. In fact, substitution ciphers can be broken by using the frequency of letters in the language.

During the 16th century, Vigenere(French) designed a cipher that was supposedly the first cipher which used an encryption key. In one of his ciphers, the encryption key was repeated multiple times spanning the entire message, and then the cipher text was produced by adding the message character with the key character modulo 26. As with the Caesar cipher, Vigenere’s cipher can also easily be broken; however, Vigenere’s cipher brought the very idea of introducing encryption keys into the picture, though it was poorly executed. Comparing this to Caesar cipher, the secrecy of the message depends on the secrecy of the encryption key, rather than the secrecy of the system.

At the start of the 19th century when everything became electric, Hebern(USA) designed an electro-mechanical contraption which was called the Hebern rotor machine. It uses a single rotor, in which the secret key is embedded in a rotating disc. The key encoded a substitution table and each key press from the keyboard resulted in the output of cipher text. This also rotated the disc by one notch and a different table would then be used for the next plain text character. This was again broken by using letter frequencies.

The Engima machine was invented by German engineer Arthur Scherbius at the end of World War I, and was heavily used by the German forces during the Second World War. Up to the Second World War, most of the work on cryptography was for military purposes, usually used to hide secret military information. However, cryptography attracted commercial attention post-war, with businesses trying to secure their data from competitors.

Questions

1. What are the countries that used cryptography?

2. Who used a form of encryption to convey secret message to his generals?

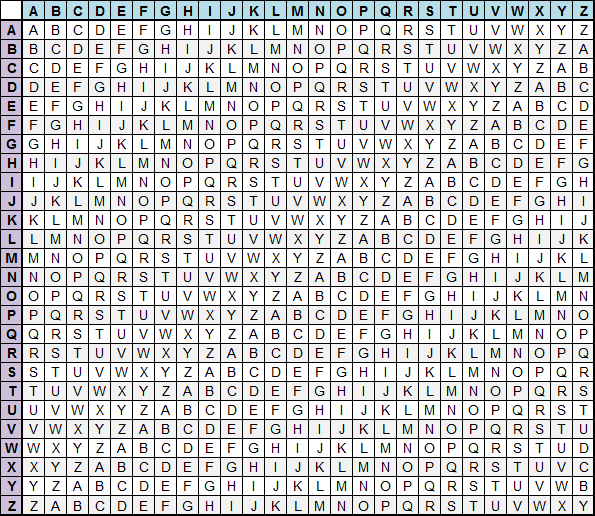
3. What are the machines that used for encrypting codes?

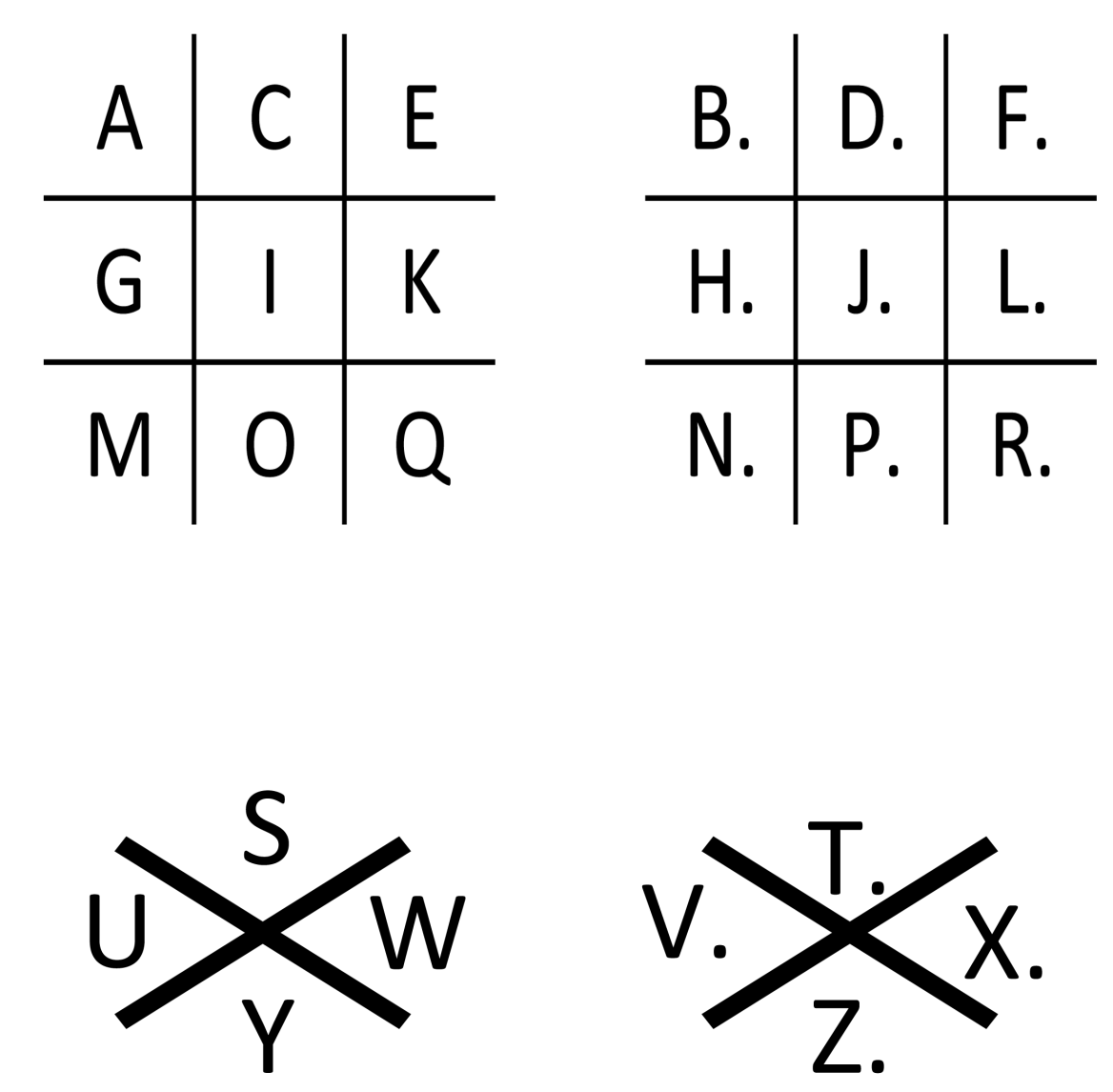
4. Who designed first cipher which used an encryption?

5. If you were Julius Caesar, what messages would you have encrypted?

6. Why do you think the Enigma machine was heavily used by the German forces

Vigenere Square





Alphabets of Olivier Levasseur

The Enigma machine

