

# Cryptography



*EMU TPS Workshop August 8 - 10, 2011*

## **A Lesson Based on the Oral History of WW II Veteran Lawrence E. Arnett**

*Written by Laura Edge and Jacqueline Crandall: August 2011*

### **Lesson Overview:**

Students will learn about the history and uses of cryptography and will understand the importance of cryptography as used in World War II. The use of cryptography will be personalized and brought to life by viewing an oral history interview of Lawrence E. Arnett, U.S. Army Cryptographer. Students will also explore early techniques for creating secret writing and will learn to encode and decode a message by creating their own letter-based code and by solving a message encoded by a classmate.

### **Objectives:**

Students will:

- Observe the human side of history as revealed through viewing the oral history interview of World War II veteran Lawrence E. Arnett
- Understand the need for coding messages during World War II
- Understand how cyptography helped determine the Allied victory in Europe
- Analyse a photo of an encrytion machine and photos taken by Lawrence Arnett while stationed in Europe
- Analyse an oral history

- Correctly use the following vocabulary words in class discussions: cryptography, encode, decode, cipher, encrypt, encryption
- Demonstrate their ability to encrypt a message by using a Caesar Cipher
- Create their own code and then encode a message in an attempt to puzzle their classmates

## **Standards:**

### **WHG ERA 7 – GLOBAL CRISIS AND ACHIEVEMENT, 1900-1945**

#### **7.1 Global or Cross-temporal Expectations**

*Analyze changes in global balances of military, political, economic, and technological power and influence in the first half of the 20th century.*

**7.1.1 Increasing Government and Political Power** – Explain the expanding role of state power in managing economies, transportation systems, and technologies, and other social environments, including its impact of the daily lives of their citizens. (See 7.3.2) (*National Geography Standard 13, p. 210*)

**7.1.2 Comparative Global Power** – Use historical and modern maps and other sources to analyze and explain the changes in the global balance of military, political, and economic power between 1900 and 1945 (including the changing role of the United States and those resisting foreign domination). (*National Geography Standard 13, p. 210*)  
28 HIGH SCHOOL SOCIAL STUDIES CONTENT EXPECTATIONS V 10/07 MICHIGAN DEPARTMENT OF EDUCATION

### **WORLD HISTORY AND GEOGRAPHY**

**7.1.4 Global Technology** – Describe significant technological innovations and scientific breakthroughs in transportation, communication, medicine, and warfare and analyze how they both benefited and imperiled humanity. (*National Geography Standard 11, p. 206*)

**7.1.5 Total War** – Compare and contrast modern warfare and its resolution with warfare in the previous eras; include analysis of the role of technology and civilians. (See 7.2.1; 7.2.3) (*National Geography Standard 13, p. 210*)

### **U.S. HISTORY AND GEOGRAPHY**

#### **USHG ERA 7 – THE GREAT DEPRESSION AND WORLD WAR II (1920-1945)**

**7.2.2 U.S. and the Course of WWII** – Evaluate the role of the U.S. in fighting the war militarily, diplomatically and technologically across the world (e.g., Germany First strategy, Big Three Alliance and the development of atomic weapons)

### **MATHEMATICS**

#### **DATA AND PROBABILITY**

**D.PR.08.03** Compute relative frequencies from a table of experimental results for a repeated event. Interpret the results using relationship of probability to relative frequency.

#### **TECHNOLOGY (National Educational Technology Standards)**

1. Students will demonstrate creative thinking, construct knowledge, and develop innovative products and processes using technology.
5. Students understand human, cultural and social issues related to technology and practice legal and ethical behavior.

**Time Required:** four class periods

**Recommended Grade Level(s):** 6-8

**Topic(s):** WWII in Europe, Cryptography, American Veterans, Supreme Headquarters Allied Expedition Force (SHAEF)

**Era:** World War II

**Preparation:**

Work with librarian to collect both print and non-print resources to be made available to support student interest in cryptography

Photocopy of a variety of cryptography puzzles

Photocopy Teacher's Guides and Analysis Tools

Library of Congress "Analyzing Oral Histories"

Library of Congress "Analyzing Photographs and Prints"

Photocopy for each student

Picture of encryption machine

Cryptography Vocabulary List

Informational page: The Caesar Cipher

Informational page: Vigenere Square

Download Oral History of Lawrence E. Arnett from Veterans History Project for viewing

Enlarge and print photos taken by Lawrence Arnett for posting in the classroom

Enlarge and print photo of General Eisenhower taken at SHAEF Headquarters on VE Day

**Materials:**

Oral History Interview of Lawrence E. Arnett (Veterans History Project)

Photos taken by Lawrence E. Arnett (Veterans History Project)

Library of Congress "Analyzing Oral Histories"

Library of Congress "Analyzing Photographs and Prints"

Handouts:

Pictures of encryption machines

Information page: The Caesar Cipher

Information page: Vigenere Square

Teacher information pages:

Enigma: A United States Air Force Academy article about this German encryption machine

A Brief History of Cryptography as found in kids.net.au

## **Resources:**

See resource table

## **Procedure:**

1. Begin the unit by referring to the picture of an encryption machine: Generate discussion regarding this machine: What is it? What was it used for? Refer to Library of Congress “Analyzing Photographs and Prints.” Secondly, refer to pictures taken by Lawrence Arnett while stationed in Europe. Again refer to “Analyzing Photographs and Prints” to generate discussion: What can we learn about Lawrence’s service to his country by viewing these pictures? As time allows, compare and contrast the VE Day Photo of Lawrence Arnett with the VE Day photo of General Eisenhower
2. Give brief overview of cryptography. Introduce vocabulary needed for understanding.
3. Show Oral History Interview of Lawrence Arnett as found on the Veterans History Project website
4. After viewing the interview, Use Library of Congress “Analyzing Oral Histories” as a guide to generate discussion
5. Read together the information about the Caesar Cipher. While working with a partner have students code a message using a Caesar Cipher.
6. Have students trade their coded messages with a classmate and attempt to decode at least one message coded by a classmate

## **Extension Activities:**

Fiction and non-fiction books about cryptography and cryptography puzzles will be made available to students for an extended period of time. Students will be encouraged to use free time to explore these resources.

Interested students may read the informational handout about the Vigenere Square and may attempt to use this tool to code and decode messages

## **Evaluation:**

Active participation in class discussions and activities

Student products include:

- Analysis of photographs page
- Analysis or oral history page
- Encoded message – made with student-created code
- Evidence of genuine attempt to decode messages encrypted by fellow students



Rubrics for these products may be designed by teacher or in teacher-student collaboration.

## Resource Table

### Cryptography

#### A Lesson Based on the Oral History of WW II Veteran Lawrence E. Arnett: An American Cryptographer in Europe

Image	Description	Citation	Permanent URL
	Interview with Lawrence E. Arnett (08-09-2011) Veterans History Project <b>Type of Resource:</b> DVD Typewritten transcript 8 Photos	Lawrence E. Arnett Collection Veterans History Project, American Folklife Center, Library of Congress	<a href="http://loc.gov/vets/">http://loc.gov/vets/</a>  To be submitted to LOC 09-2011
	General Dwight D. Eisenhower, Supreme Allied Commander (left) makes announcement of German unconditional surrender at SHAEF Forward Headquarters, Reims, France.	Title: General Dwight D. Eisenhower, Supreme Allied Commander (left) makes announcement of German unconditional surrender	<a href="http://hdl.loc.gov/loc.pnp/cph.3c01108">http://hdl.loc.gov/loc.pnp/cph.3c01108</a>  Permanent URL: <a href="http://www.loc.gov/picture/item/90709883/">http://www.loc.gov/picture/item/90709883/</a>
	Photo and newspaper article about the Enigma machine used by the German Luftwaffe during World War II. (U.S. Air Force photo)	USAFS: Colorado Springs "Academy gains a piece of WWII crypto history"  Posted 5/17/2011	<a href="http://www.usafa.af.mil/news/story.asp?id=123256212">http://www.usafa.af.mil/news/story.asp?id=123256212</a>
	Cryptography: Encyclopedia entry World War II Cryptography Classical Cryptography Algorithms, Encryption	kids.net.au "Cryptography"	<a href="http://encyclopedia.kids.net.au/page/cr/Cryptography">http://encyclopedia.kids.net.au/page/cr/Cryptography</a>
	<b>The Abraham Lincoln Papers at the Library of Congress</b> Series 1. General Correspondence. 1833-1916. John Slight to Abraham Lincoln, Monday, March 04, 1861 (System of cryptographic writing) – Transcription	American Memory Library of Congress  John Slight to Abraham Lincoln, Monday March 4, 1861 (System of Cryptographic Writing)	<a href="http://memory.loc.gov/cgi-bin/query/r?ammem/mal:@field(DOCID+@lit(d0777400))">http://memory.loc.gov/cgi-bin/query/r?ammem/mal:@field(DOCID+@lit(d0777400))</a>

	<p>Library of Congress Teacher Resources</p> <p><b>Analyzing Photographs and Prints</b></p>	<p>Analyzing Photographs and Prints <i>Library of Congress teacher resource</i> Teacher's Guide Analyzing Photographs &amp; Prints Guide students with the sample questions as they respond to a primary source.</p>	<p><a href="http://www.loc.gov/teachers/usingprimarysources/resources/Analyzing_Photos_and_Prints.pdf">http://www.loc.gov/teachers/usingprimarysources/resources/Analyzing_Photos_and_Prints.pdf</a></p>
	<p>Library of Congress Teacher Resources</p> <p><b>Analyzing Oral Histories</b></p>	<p>Analyzing Oral Histories <i>Library of Congress teacher resource</i> Teacher's Guide Analyzing Oral Histories Guide students with the sample questions as they respond to a primary source.</p>	<p><a href="http://www.loc.gov/teachers/usingprimarysources/resources/Analyzing_Oral_Histories.pdf">http://www.loc.gov/teachers/usingprimarysources/resources/Analyzing_Oral_Histories.pdf</a></p>

## Cryptography Vocabulary List

<b>cryptography</b>	secret writing  the enciphering and deciphering of messages in secret code  <b>the computerized encoding and decoding of information</b>
<b>encode</b>	<b>to convert (a message) into code</b>
<b>decode</b>	<b>to convert a coded message into intelligible form</b>  <b>to recognize and interpret</b>
<b>cipher</b>	<b>a method of transforming a text in order to conceal its meaning</b>  <b>to code</b>
<b>encrypt</b>	to change information from one form to another, especially to hide its meaning
<b>encryption</b>	to convert a message into cipher

# Cryptography<sup>1</sup>

**Cryptography** (from [Greek](#) *kryptós*, "hidden", and *gráphein*, "to write") is generally understood to be the study of the principles and techniques by which information can be translated into a "garbled" version that is difficult for an unauthorized person to read, while still allowing the intended reader to convert the resulting [gobbledygook](#) back into the original information. In fact, cryptography covers rather more than merely encryption and decryption. It is, in practice, a specialized branch of [information theory](#) with substantial additions from other branches of mathematics, and from such sources as [Machiavelli](#), [Sun Tzu](#), and [Clausewitz](#)[?]. The term [cryptology](#) has sometimes been used instead of cryptography for this field; but there is some tension between these two lexicographic schools. There is also some tension between fans of two spellings of cypher (the alternate is cipher). In English, the cypher spelling has historical pride of place. This and related articles in the Wikipedia are often revised by those with strong opinions on the spelling question.

Unsurprisingly, the study of hiding messages from others has been accompanied by the study of how to read such messages when one is *not* the intended receiver; this area of study is called [cryptanalysis](#). People involved in such work, and with cryptography in general, are known as cryptographers (or for those in the other school, **cryptologists**).

The original information being sent from one person (or organization) to another is usually called the *plaintext*. [Encryption](#) is the plaintext-to-garble conversion, and [decryption](#) is the garble-to-plaintext conversion. A major class of encryption technique is called [encoding](#) (yielding *codetext*), after which the receiver decodes the codetext. The other major class is called [enciphering](#) (yielding, naturally, *cyphertext*), after which the receiver decyphers the cyphertext. The exact operation of the encryption and decryption, for all schemes with any pretense to security, is controlled by one or more [keys](#).

## Table of contents

- [1 Overview: goals](#)
- [2 Classical Cryptography](#)
- [3 World War II Cryptography](#)
- [4 Modern Cryptography](#)
  - [4.1 non-secret encryption](#)
- [5 Some algorithms of various kinds](#)
  - [5.1 Hash functions, aka message digest functions, cryptographic hash functions](#)
  - [5.2 open source crypto systems \(algorithms + protocols + system design\)](#)
  - [5.3 Public key / private key encryption algorithms \(aka asymmetric key algorithms\)](#)
  - [5.4 Secret key algorithms \(aka symmetric key algorithms\)](#)
  - [5.5 Pseudo-random number generators](#)
  - [5.6 Anonymous communication](#)
  - [5.7 Terminology](#)
- [6 Further Reading](#)
- [7 Related topics](#)

## Overview: goals

Cryptography has four main goals, though they are nearly always concealed beneath a blanket of confusing 'marketing speak' in commercial products. And behind a fog of rumor and myth as well. Examining any proposed crypto system with these basic functions in mind, and ignoring the marketing blather, will be a very useful exercise for those interested in cryptography in the real world. They are:

1. message *confidentiality*: Only the authorised recipient should be able to extract the contents of the message from its encrypted form. In addition, it should not be possible to obtain information about the message contents (such as a statistical distribution of certain characters) as this makes cryptanalysis easier.
2. message *integrity*: The recipient should be able to determine if the message has been altered during transmission.
3. sender *authentication*: The recipient should be able to identify the sender, and verify that the purported sender actually did send the message.
4. sender *non-repudiation*: The sender should not be able to deny sending the message.

Not all cryptographic systems or algorithms achieve all of the above goals, or are even intended to. Poorly designed, or poorly implemented, crypto systems achieve them only by accident or bluff or lack of interest on the part of the opposition, and users can and regularly do reduce even well designed and implemented crypto systems to the security equivalent of Swiss cheese. But even with well designed, well implemented, and properly used crypto systems, some goals aren't practical (or desirable) in some contexts. For example, the sender of the message may want to be anonymous, or the system may be intended for an environment with limited computing resources, or confidentiality might not matter.

In addition, some confusion may arise in a crypto system design regarding whom we are referring to when speaking of the "sender" or "recipient"; some examples for real crypto systems in the modern world include:

1. a computer program on a local system,
2. a computer program on a 'nearby' system which 'provides security services' for users on other nearby systems,
3. or -- what most people assume is "obviously" meant -- a human being (usually understood as one 'at a keyboard' to actively send or receive). Even in such cases, the human does not actually encrypt or sign or decrypt or authenticate anything in modern cryptographic systems. At most, when all is right in the world, the user instructs a computer program to encrypt or sign or decrypt and authenticate, or ... and it does so, properly and securely. This buffering of human action from actions which are presumed (without much consideration) to have 'been done by a human' is a source of problems in crypto system design, implementation, and use. Such problems are often quite subtle and correspondingly obscure. Generally, even to practicing cryptographers with knowledge, skill, and good engineering sense.

When confusion on these points is present (at the design stage, during implementation, or by a user after installation), unintended failures in reaching each of the stated goals can occur quite easily, often without notice to any human involved, and even given perfect algorithms, superb and provably secure system design, and error free implementation. Such failures are most often due to extra-cryptographic issues; each such failure demonstrates that good algorithms, good protocols, good system design, and

---

<sup>1</sup> <http://encyclopedia.kids.net.au/page/cr/Cryptography>



good implementation do not alone, nor in combination, provide 'security'. Instead, careful thought is required regarding the entire system design and its use in actual production - too often, this is absent or insufficient in practice with real-world crypto systems.

Although cryptography has a long and complex history, it wasn't until the [19th century](#) that it developed anything more than ad hoc approaches to either [cryptanalysis](#) (eg, [Charles Babbage's](#) Crimean War era work on mathematical cryptanalysis of polyalphabetic cyphers, repeated publicly rather later by the Prussian Kasiski) or encryption (eg, [Auguste Kerckhoffs'](#) writings in the later 19th century). An increasingly mathematical trend accelerated up to [World War II](#) (notably in [William F. Friedman's](#) application of statistical techniques to cryptography and in [Marian Rejewski's](#) initial break into the German Army's version of the [Enigma](#) system). Both cryptography and cryptanalysis have become far more mathematical since WWII. Even then, it has taken widely available computers, and the [Internet](#), to bring effective cryptography into common use by anyone other than national governments or similarly sized enterprises.

## Classical Cryptography

The earliest known use of cryptography is found in non-standard [hieroglyphics](#) on monuments from Egypt's Old Kingdom (ca 4000 years ago). These are not thought to be serious attempts at secret communications, however, but rather to have been attempts at mystery, intrigue, or even amusement for literate onlookers. Each of which has been, intermittently, still another use of cryptography, or of something that looks (impressively if misleadingly) like it. Later, [Hebrew](#) scholars made use of simple [substitution ciphers](#) (such as the [Atbash cipher](#)) beginning perhaps around 500 to 600 BCE. Cryptography has a long tradition in religious writing likely to offend the dominant culture or political authorities. Perhaps the most famous is the 'Number of the Beast' from the book of Revelations in the Christian New Testament. 666 is almost certainly a cryptographic (ie, encrypted) way of concealing a dangerous reference; many scholars believe it's a way of referring to Rome, or Nero, (and so to Roman policies of persecution of Christians) that would be understood by the initiated (who 'had the codebook') and yet be safe (or at least somewhat deniable and so less dangerous) if it came to the attention of those authorities. At least for orthodox Christian writing, the need for such concealment ended with Constantine's conversion and the adoption of Christianity as the official religion of the Empire.

The Greeks of Classical times are said to have known of cyphers (eg, the [scytale](#) transposition cypher claimed to have been used by the Spartan military). Herodotus tells us of secret messages physically concealed beneath wax on wooden tablets or as a tattoo on a slave's head concealed by regrown hair (see [secret writing](#); these are not properly examples of cryptography). The Romans certainly did (eg, the [Caesar cipher](#) and its variations). There is ancient mention of a book about Roman military cryptography (especially Julius Caesar's); it has been, unfortunately, lost. Cryptography became (secretly) important still later as a consequence of political competition and religious analysis. For instance, in Europe during and after the Renaissance, citizens of the various Italian states, including the Papacy, were responsible for substantial improvements in cryptographic practice (eg, polyalphabetic cyphers invented by [Leon Alberti](#)? ca 1465). And in the Arab world, religiously motivated textual analysis of the Koran led to the invention of the [frequency analysis](#) technique for breaking monoalphabetic substitution cyphers sometime around 1000 CE.

Both cryptography, [cryptanalysis](#), and secret agent betrayal featured in the [Babington plot](#) during the reign of Queen [Elizabeth I](#) which led to the execution of Mary, Queen of Scots. And an encrypted message from the time of the Man in the Iron Mask (decrypted around 1900 by [ϕtienne Bazeries](#)?) has shed some, regrettably non-definitive, light on the identity of that legendary, and unfortunate, prisoner. Cryptography, and its misuse, was involved in the plotting which led to the execution of [Mata Hari](#) and even more reprehensibly in the travesty which led to [Dreyfus' conviction](#) and imprisonment, both in the early [20th century](#). Fortunately, cryptographers were also involved in setting Dreyfus free; Mata Hari, in contrast, was shot.

Mathematical cryptography leaped ahead (mostly secretly) after [World War I](#). Marian Rejewski, in [Poland](#), attacked and 'broke' the early German Army [Enigma](#) system (an electromechanical rotor cypher machine) using theoretical mathematics in [1932](#). The break continued up to '39, when changes in the way the German Army's Enigma machines were used required more resources than the Poles could deploy. His work was extended by [Alan Turing](#), Gordon Welchman, and others at [Bletchley Park](#) beginning in [1939](#), leading to sustained breaks into several other of the Enigma variants and the assorted networks for which they were used. [US Navy](#) cryptographers (with cooperation from British and Dutch cryptographers after 1940) broke into several [Japanese Navy](#)? crypto systems. The break into one of them famously led to the US victory in the [Battle of Midway](#). A US Army group, the [SIS](#), managed to break the highest security Japanese diplomatic cypher system (an electromechanical 'stepping switch' machine called [Purple](#) by the Americans) before WWII began. The Americans referred to the intelligence resulting from cryptanalysis, perhaps especially that from the Purple machine, as ['Magic'](#). The British eventually settled on ['Ultra'](#) for intelligence resulting from cryptanalysis, particularly that from message traffic encyphered by the various Enigmas. An earlier British term for Ultra had been 'Boniface'.

## World War II Cryptography

By [World War II](#) mechanical and electromechanical cryptographic cypher machines were in wide use, although where these were impractical manual systems continued to be used. Great advances were made in both practical and mathematical cryptography in this period, all in secrecy. Information about this period has begun to be declassified in recent years as the official 50-year (British) secrecy period has come to an end, as the relevant US archives have slowly opened, and as assorted memoirs and articles have been published.

The Germans made heavy use (in several variants) of an electromechanical rotor based cypher system known as [Enigma](#), the Japanese Foreign Office used an independently developed electrical stepping switch based system (called [Purple](#) by the US), and also used several similar machines for attaches in some Japanese embassies. One of these was called the 'M-machine' by the US, another was referred to as 'Red'. All were broken, to one degree or another by the Allies. The German military also deployed several mechanical implementations of [one-time pads](#)? Bletchley Park called them the [Fish cyphers](#)? and [Max Newman](#) and colleagues designed and deployed the world's first programmable electronic computer, the [Colossus](#), to help with those cypher systems.

Other cypher machines used in WWII included the British Type X and the American [SIGABA](#); both were electromechanical rotor designs similar in spirit to the Enigma. Neither is known to have been broken by anyone during the war.

## Modern Cryptography

The era of modern cryptography really begins with [Claude Shannon](#), arguably the father of mathematical cryptography. In [1949](#) he published the paper [Communication Theory of Secrecy Systems](#) (<http://www3.edgenet.net/dcowley/docs>) in the Bell System Technical Journal and a little later the book, Mathematical Theory of Communication, with Warren Weaver. These, in addition to his other works on [information and communication theory](#), established a solid theoretical basis for cryptography and for cryptanalysis. And with that, cryptography more or less disappeared into secret government communication organisations such as the [NSA](#). Very little work was again made public until the mid '70s, when everything changed.

[1976](#) saw two major public (ie, non-secret!) advances. First was the [DES](#) (Data Encryption Standard) submitted by [IBM](#), at the invitation of the National Bureau of Standards (now NIST), in an effort to develop secure electronic communication facilities for businesses such as banks and other large financial organizations. After 'advice' and modification by the [NSA](#), it was adopted and published as a [FIPS](#) Publication (Federal Information Processing Standard) in [1977](#) (currently at FIPS 46-3). It has been made effectively obsolete by the adoption in 2001 of the Advanced Encryption Standard, also a NIST competition, as FIPS 197. DES was the first publicly accessible cypher algorithm to be 'blessed' by a national crypto agency such as NSA. The release of its design details by NBS stimulated an explosion of public and academic interest in cryptography. DES and more secure variants of it (such as [3DES](#), see FIPS 46-3) are still used today, although DES was officially supplanted by [AES](#) (Advanced Encryption Standard) in [2001](#) when NIST announced the selection of Rijndael, by two Belgian cryptographers, as the AES. DES remains in wide use nonetheless, having been incorporated into many

Jacqueline Crandall ([leejacqu@msu.edu](mailto:leejacqu@msu.edu)) and Laura Edge ([lawe@umich.edu](mailto:lawe@umich.edu))

national and organizational standards. However, it has been broken (by the [Electronic Frontier Foundation](#), a cyber civil rights group -- the story is in *Cracking DES*, published by O'Reilly and Associates) -- and it should not be used in new crypto system designs.

Second, and perhaps even more important, was the publication of the paper [New Directions in Cryptography](#) (<http://citeseer.nj.nec.com/340126>) by [Whitfield Diffie](#) and [Martin Hellman](#). This paper introduced a radically new method of distributing cryptographic keys, which went far toward solving one of the fundamental problems of cryptography, key distribution. It has become known as [Diffie-Hellman key exchange](#). The article also seems to have stimulated the almost immediate public development of a new class of enciphering algorithms, the [asymmetric key algorithms](#).

Prior to that time, all useful modern encryption algorithms had been [symmetric key algorithms](#), in which the same [cryptographic key](#) is used with the underlying algorithm by both the sender and the recipient who must both keep it secret. All of the electromechanical machines used in WWII were of this logical class, as were the Caesar and Atbash cyphers and essentially all cypher and code systems throughout history. The 'key' for a code is, of course, the codebook, which must likewise be distributed and kept secret.

Of necessity, a key in every such system had to be exchanged between the communicating parties in some secure way prior to any use of the system (the term usually used is 'via a secure channel') such as a trustworthy courier with a briefcase handcuffed to a wrist, or face-to-face contact, or a loyal carrier pigeon. This requirement rapidly becomes unmanageable when the number of participants increases beyond some small number, or when (really) secure channels aren't available for key exchange. In particular, a separate key is required for each communicating pair if other parties are not to be able to decrypt their messages. A system of this kind is also known as a [private key, secret key, or conventional key](#) cryptosystem. D-H key exchange (and succeeding improvements) made operation of these systems much easier, and more secure, than had ever been possible before.

In contrast, in [asymmetric key](#) encryption, there is a pair of mathematically related keys for the algorithm, one of which is used for encryption and the other for decryption. Some, but not all, of these algorithms have the additional property that one of the keys may be made public since the other cannot be (by any currently known method) deduced from the 'public' key. The other key in these systems is kept secret and is usually called the 'private' key. An algorithm of this kind is known as a [public key / private key algorithm](#), although the term [asymmetric key cryptography](#) is preferred by those who wish to avoid the ambiguity of using that term for all such algorithms, and to stress that there are two distinct keys with different secrecy requirements.

As a result, only one key pair is now needed per recipient (regardless of the number of senders) as possession of a public key (by anyone whatsoever) does not compromise the 'security' of the algorithm so long as the corresponding private key is not known to any attacker (effectively this means not known to anyone except the sender). These algorithms made practical, and possible, the widespread deployment of high quality crypto systems which could be used by anyone. This gave government crypto organizations worldwide a severe case of heartburn; for the first time, those outside that fraternity might have access to cryptography that wasn't readily breakable by the snooping side of those organizations. Considerable controversy, and conflict, began almost immediately. It has not yet died down. (See S Levy's *Crypto* for a journalist's account of the policy controversy in the US).

Note, however, that it has NOT been proven, for any of the good public/private asymmetric key algorithms, that a private key cannot be deduced from a public key (or vice versa). However, informed observers believe it to be currently impossible (and perhaps forever impossible) for the 'good' asymmetric algorithms; no workable deduction techniques have been publicly shown for any of them. Note also that some asymmetric key algorithms have been quite thoroughly broken, just as many symmetric key algorithms have; there is no special magic attached to using two keys.

In fact, some of the well respected, and most widely used, public key / private key algorithms can be broken by one or another cryptanalytic attack and so, like most encryption algorithms, the protocols within which they are used must be chosen and implemented carefully. \_All\_ of them can be broken if the key length used is short enough to permit practical brute force key search; indeed this is true of all encryption algorithms using keys, regardless of their type.

This is an example of the fundamental problem for those who wish to keep their communications secure; they must choose a crypto system (algorithms + protocols + operation) that resists all attack from any attacker. There being no way to know who those attackers might be, nor what resources they might be able to deploy, nor what advances in cryptanalysis (or its associated mathematics) might in future occur, users may ONLY do the best they know how, and then hope. In practice, for well designed / implemented / used crypto systems, this is believed by informed observers to be enough, and possibly even enough for all(?) future attackers. Distinguishing between well designed / implemented / used crypto systems and crypto trash is another, quite difficult, problem for those who are not themselves expert cryptographers. It is even quite difficult for those who are.

## non-secret encryption

Asymmetric key cryptography, D-H key exchange, and the best known of the public key / private key algorithms (ie, what is usually called the RSA algorithm), all seem to have been developed at a UK intelligence agency before the public announcement by Diffie and Hellman in '76. [GCHQ](#) has released documents claiming that they had developed public key cryptography before the publication of Diffie and Hellman's paper. Various classified papers were written at GCHQ during the [1960s](#) and [1970s](#) which eventually led to schemes essentially identical to [RSA](#) encryption and to [Diffie-Hellman](#) key exchange in [1973](#) and [1974](#). Some of these have now been published, and the inventors (James Ellis, Clifford Cocks, and Malcolm Williamson) have made public (some of) their work.

Some algorithms of various kinds

## [Hash functions](#), aka message digest functions, cryptographic hash functions

- [MD5](#)
- [SHA-1](#)
- [RIPEMD-160](#)
- [Tiger](#)

## open source crypto systems (algorithms + protocols + system design)

- [PGP](#)

Jacqueline Crandall ([leejacqu@msu.edu](mailto:leejacqu@msu.edu)) and Laura Edge ([lawe@umich.edu](mailto:lawe@umich.edu))

- [GPG](#)
- [SSH](#)
- [IPSec / Free S/WAN\[?\]](#)

## Public key / private key encryption algorithms (aka [asymmetric key algorithms](#))

- [Diffie-Hellman](#)
- [El Gamal\[?\]](#)
- [Elliptic curve cryptography](#)
- [RSA](#)

## Secret key algorithms (aka [symmetric key algorithms](#))

- [Enigma](#) (WWII German rotor cypher machine -- many variants, many users)
- [Purple](#) (WWII Japanese Foreign Office cypher machine)
- [SIGABA](#) (WWII US cypher machine)
- [JN-25\[?\]](#) (WWII Japanese Navy superencyphered code)
- [One-time pad](#) (Vernam and Mauborgne, patented mid-'20s)
- [Data Encryption Standard](#) (DES, FIPS 46-3, 1976)
- [Lucifer cipher\[?\]](#) (IBM, early 1970s; modified to become DES)
- [RC4 cipher](#) (one of a series by Ron Rivest of MIT)
- [Blowfish](#) (by Bruce Schneier, et al)
- [International Data Encryption Algorithm](#) (IDEA -- J Massey and X Lai)
- [Advanced Encryption Standard](#) (AES, FIPS 197, 2001 -- by Daemen and Rijmen)
- [Twofish](#) (AES finalist, by Schneier et al)
- [RC6](#) (AES finalist, by Rivest et al)
- [MARS\[?\]](#) (AES finalist, by Don Coppersmith et al)
- [Serpent](#) (AES finalist, by Ross Anderson et al)
- [Iraqi Block Cipher](#) (IBC)

## [Pseudo-random number generators](#)

- [Blum Blum Shub](#)
- [Yarrow](#) (by Schneier, et al)
- [Fortuna](#) (by Schneier, et al)
- [ISAAC](#)

## Anonymous communication

- [Dining cryptographers protocol](#) (by David Chaum)
- [Anonymous remailer](#)

## Terminology

- [Cryptographic key](#)
- [Cipher](#)
- [Code](#)
- [Brute force attack](#)
- [Dictionary attack](#)
- [Unicity distance](#)

## Further Reading

- General note on cryptographic references: There is a great amount of myth and misunderstanding in wide circulation about topics cryptographic. Some is grossly wrong, some is 'merely' subtly misleading, much of it is plausible to the crypto newcomer and even to the somewhat experienced. There is also a very great selection of poorly done, non-secure cryptographic software on the market (purchaseware, shareware, freeware, journalware, xyzware). Readers, buyers, and users should exercise \_substantially\_ more than the usual caution lest they lose one, two, or all of the reasons they have bothered with cryptography at all (see the article above for the goals of cryptography). At the time this sentence was written, each of the following references is reliable. Mostly. Consider that none covers up\_to\_date secret government cryptography (at minimum, publishing schedules do not permit it, more generally NSA and brethren don't talk), none is even complete for material available before publication, and none is error free. All of this, plus individual differences in comprehension of a complex field, may produce considerable distortions in your understanding of the current state of the art in cryptography. Nevertheless, try these references first if you wish to minimize those distortions.
- [The Beginner's Guide to Cryptography](http://www.murky.org/cryptography/index.shtml) (<http://www.murky.org/cryptography/index.shtml>) - This website gives a (quite) elementary overview of a few basic areas of cryptography.
- [Ferguson, Niels](#), and [Schneier, Bruce](#) - *Practical Cryptography*, Wiley, 2003, [ISBN 0471223573](#). Up to date cryptography reference. Covers both algorithms and protocols. This is an in depth consideration of one cryptographic problem, including paths not taken and some reasons why. Most of the material is not otherwise available in a single source. Some is not otherwise available. In a sense, a follow-up to 'Applied Cryptography'.
- [Schneier, Bruce](#) - *Applied Cryptography*, 2 ed, Wiley, [ISBN 0471117099](#). The best single volume available covering modern cryptographic practice and possibilities. About as comprehensive as a single volume could have been. Not overly mathematical, well written, and so accessible -- mostly -- to the non-technical.
- [Schneier, Bruce](#) - *Secrets and Lies*, Wiley, [ISBN 0471253111](#), a discussion of the context within which cryptography and cryptosystems work. Meta-cryptography, if you will. Required reading for would be cryptographers, and nearly so for all cryptography users.
- [Ross Anderson](#) -- *Security Engineering*, advanced coverage of computer security issues, including cryptography, by one of its foremost practitioners, and most likely its best writer.
- Bamford, James - *The Puzzle Palace : A Report on America's Most Secret Agency* [ISBN 0140067485](#), and the more recent "Body of Secrets". The best of a quite small group of books about NSA. Most are inadequate, and untrustworthy, for various reasons.
- A. J. Menezes, P. C. van Oorschot and S. A. Vanstone - *Handbook of Applied Cryptography* [ISBN 0849385237](#) ([online version](http://cacr.math.uwaterloo.ca/hac/) (<http://cacr.math.uwaterloo.ca/hac/>)). Equivalent to Applied Cryptography in many ways, but seriously mathematical.
- Kahn, David - *The Codebreakers* [ISBN 0684831309](#) The best available single volume source for cryptographic history, at least for events up to the mid '60s. The added chapter on more recent developments (in the most recent edition) is regrettably far too thin. See also his other publications on cryptography which have been uniformly excellent.
- Piper, Fred and Sean Murphy - *Cryptography : A Very Short Introduction* [ISBN 0192803158](#) This book quickly sketches out the major goals, uses, methods, and developments in cryptography.
- Singh, Simon - *The Code Book* [ISBN 1857028899](#). An anecdotal introduction to the history of cryptography, but much better than such an approach might be expected to produce. Covers more recent material than does Kahn's The Codebreakers. Well written. Sadly, the included cryptanalytic contest has been won and the prize awarded; the cyphers are still worth having a go at, however.

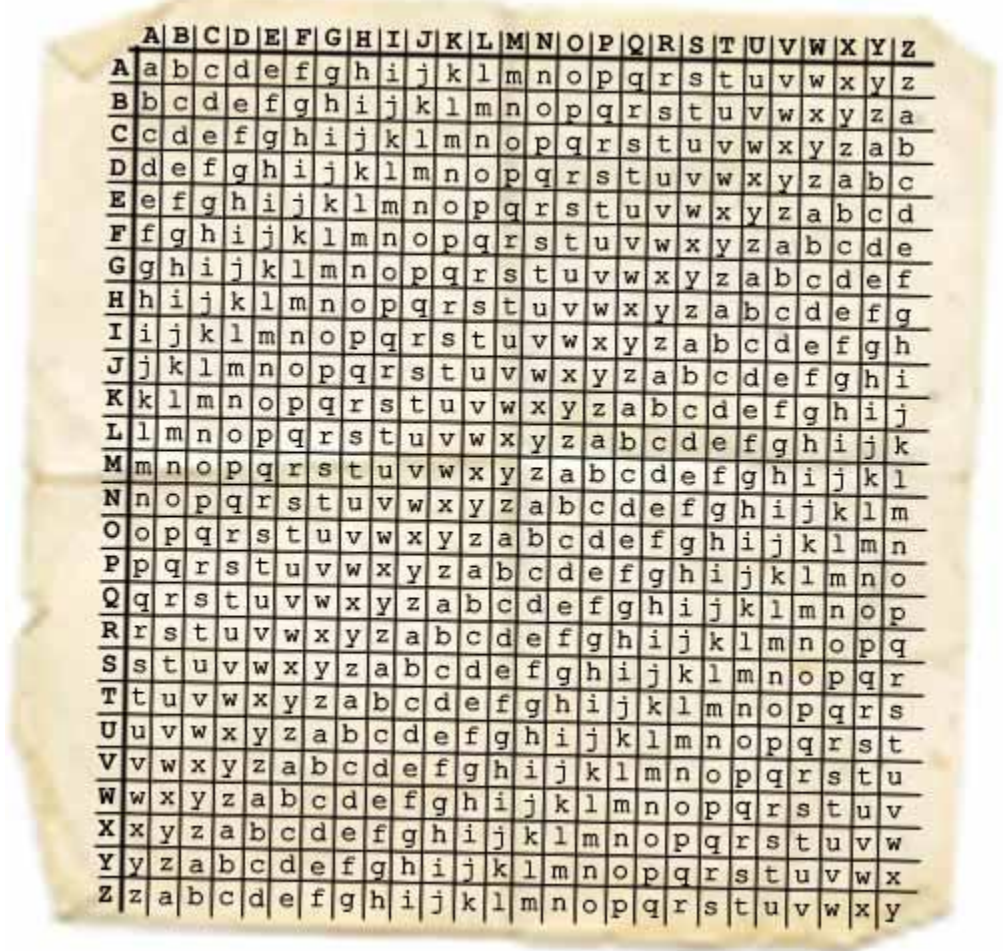
**Related topics** [Echelon](#), [Enigma](#), [Espionage](#), [IACR](#), [Purple code](#), [Ultra](#), [Security engineering](#), [SIGINT](#), [Steganography](#), [Cryptographers](#), [SSL](#), [Quantum Cryptography](#), [Crypto-anarchism](#), [Cypherpunk](#)

---

All Wikipedia text is available under the terms of the GNU Free Documentation License

# Ciphering<sup>2</sup>

## Vigenere Square



See how the alphabet is shifting to the left as you go down?

### How to use the Vigenere Cipher

First, you and your spy ring (fellow spies you communicate with) need to agree on a keyword or a key phrase, to code and decode the sentences that you send.

Say that you choose the word "ESPIONAGE". Now you and your fellow spies have both the Vigenere

---

<sup>2</sup> <http://www.topspysecrets.com/vigenere-cipher.html>

cipher square and the keyword, so you have what you need to code and decode sentences.

## Encoding

To see how it works, it's best to give it a try. So, let's code the sentence "MEET ME AFTER SCHOOL".

First, write out the sentence without the spaces in between, and write the keyword below it, repeating the characters until it's as long as the sentence you're encoding:

M	E	E	T	M	E	A	F	T	E	R	S	C	H	O	O	L
E	S	P	I	O	N	A	G	E	E	S	P	I	O	N	A	G

Then, for each combination, find the character that is on the intersection of the **column** (top character) and the **row** (bottom character). To get the coded character for the top letter (the first letter of the sentence "M") you go down the rows until you reach the row that has the bottom character (the first letter of the word ESPIONAGE, "E"). The character that's on the intersection is "Q".

M	E	E	T	M	E	A	F	T	E	R	S	C	H	O	O	L
E	S	P	I	O	N	A	G	E	E	S	P	I	O	N	A	G
q																

Ok, one more time. Top character is "E", bottom character is "S". Going down the column "E", until you reach row "S", you find the coded letter "W". And so on and so forth.

M	E	E	T	M	E	A	F	T	E	R	S	C	H	O	O	L
E	S	P	I	O	N	A	G	E	E	S	P	I	O	N	A	G
q	w	t	b	a	r	a	l	x	i	j	h	k	v	b	o	r

The coded sentence is: QWTBA RALXI JHKVB OR  
(written down in blocks of 5 chars, a usual way of writing down coded messages).

## Decoding

Now what do you do when you receive that message? Well, it's more of the same, just the other way around.

Write the coded text, and below it the keyword, repeating as long as the coded text is.

q	w	t	b	a	r	a	l	x	i	j	h	k	v	b	o	r
E	S	P	I	O	N	A	G	E	E	S	P	I	O	N	A	G

Now, for each combination, do the following. Find the row for the bottom character. In our example, "E" (first letter of "ESPIONAGE"). Then look through that row until you find the character in the top row, in this case "q". Then go up to see the letter that is at the top of that column. The column that has the letter "q" is the "M" column.

Next character to look for is the letter "w" in the row "S". The letter "w" on that row can be found in the column "E".

And so on and so forth:

q	w	t	b	a	r	a	l	x	i	j	h	k	v	b	o	r
E	S	P	I	O	N	A	G	E	E	S	P	I	O	N	A	G
M	E	E	T	M	E	A	F	T	E	R	S	C	H	O	O	L

### Some practice for you

Here is a coded message to practice the Vigenere cipher. The keyword to decode it with is "COMPLETE". Once you learned what the coded message means, **do it!**

TSOGF MMEIS ZIDJH VVCBH ACLIE FQID

A Box Like This May Have Saved Millions of Lives During World War II  
What is it?



3

---

<sup>3</sup> From the collection of the United States Air Force Academy  
<http://www.usafa.af.mil/shared/media/photodb/photos/110516-F-YY717-008.JPG>

Jacqueline Crandall ([leejacqu@msu.edu](mailto:leejacqu@msu.edu)) and Laura Edge ([lawe@umich.edu](mailto:lawe@umich.edu))



## The Caesar Cipher

Julius Caesar used cryptology to communicate with his army. The type of encryption he employed is called the "Caesar Cipher" or the "Caesar Shift Cipher." This is a simple code that is based on shifting letters in a message in an attempt to make the message secure or "secret."

### Example:

Using a Caesar Shift of three letters to the right (+3) the quote, "I came, I saw, I conquered" would be encrypted as:

L FDPH L VDZ L FRQTXHUHG

Using a Caesar Shift of -13, the encrypted message becomes:

V PNZR V FNJ V PBADHRERQ

## Assignment

### Can You Break the Code?

Work with your group to decode a Crypto-Quote.<sup>4</sup>

---

<sup>4</sup> Free, Printable Cryptogram Puzzles! As found at <http://www.cryptquote-cryptogram-puzzles.com/>



This Enigma machine, Serial No. 01182, was used by the German Luftwaffe during World War II. (U.S. Air Force photo/

## Academy gains a piece of WWII crypto history

Posted 5/17/2011

5/17/2011 - **U.S. AIR FORCE ACADEMY, Colo.** -- On a table in Dr. Barry Fagin's office sits a plain gray box that weighs about 30 pounds and smells of machinery and dusty paper. Its nondescript appearance, however, belies its significance: in the right hands, a box like this may have saved millions of lives during World War II.

The box holds a Luftwaffe Enigma machine, Serial No. 01182, now on permanent loan to the Air Force Academy's Department of Computer Science from the National Cryptologic Museum at Fort George G. Meade, Md.

Dr. Steve Fulton, the Academy's assistant professor of computer science currently on leave from the Department of Defense, arranged for the loan to the Air Force Academy after finding out that a similar machine was on permanent loan to the U.S. Military Academy, Dr. Fagin said.

Enigma was originally designed in the 1920s to allow secure communication between banks, but the machines never took off in that role. The German government, however, saw the value of what was, at the time, an unbreakable code.

"To borrow a line from the Remington commercial, they liked it so much they bought the company," Dr. Fagin said.

Enigma machines like those used by the Luftwaffe had strong encryption, even by today's standards. If a would-be decrypter did not know the Enigma plugboard's wiring configuration, he would have to "brute force" his way through 380-bit encryption.

"The [key space](#) is impossibly huge -- greater than all the electrons in the solar system," Dr. Fagin said.

In theory, Enigma should have ensured secure communications for Germany throughout the war. In practice, the Polish had broken the Enigma code twice: once, almost seven years before the German incursion that sparked World War II on Sept. 1, 1939, and again after the Germans introduced a fourth and fifth rotor to their Enigma machines.

Dr. Fagin said the project to decrypt German communications, called Ultra, was one of the Allies' most important strategic achievements. Sir Harry Hinsley, the historian of British Intelligence in World War II, credited Ultra with shortening the war by two to four years in his 1993 book, "British Intelligence in the Second World War."

Lax information security measures provided inroads to Project Ultra's success. Some of the factors that allowed the Allies to break Enigma included early training manuals that included both the plain text, the cipher text and the message key used to encode the text, along with the use of easily guessed keys or keys that mapped to the Enigma keyboard's layout, according to Marian Rejewski, who broke the Enigma code in 1932.

---

<sup>5</sup> <http://www.usafa.af.mil/news/story.asp?id=123256212>

As a result, Dr. Fagin said, the Allies had access to all communication between German high command and the German navy, or Kriegsmarine, the last two years of the war, as well as many other encoded messages.

"(Field Marshal Bernard) Montgomery was reading all of (Field Marshal Erwin) Rommel's communications," Dr. Fagin said. "He knew all about Rommel's supply problems and all his planned moves."

The Academy's Enigma machine needs some repairs, Dr. Fagin said. Once it's fixed, the Computer Science department plans to use the device in its Introduction to Computing and Cryptography classes.

"It will eventually go on permanent display, where we anticipate it will be hands-on," Dr. Fagin added. "It will also serve as a reminder of our heritage: code making, code breaking and cryptology's contributions to the war effort. We hope it will inspire and motivate cadets to think about information security and cyberspace."

### KEY SPACES EXPLAINED

The key space of an encryption key is a measure of the number of possible combinations. A 1-bit key would have two possible combinations, while a 2-bit key would have four combinations, and a 3-bit key would have eight combinations. Each additional bit doubles the number of possible encryption combinations.

Enigma had approximately 380-bit encryption, factoring in both the reels and the number of possible plugboard combinations. This works out to approximately  $10^{114}$  possible combinations. By way of comparison, the certificates on Common Access Cards use 160-bit keys ( $10^{48}$  combinations), and e-commerce websites use 256-bit encryption ( $10^{77}$  combinations). Today, a key considered safe from brute-force decryption generally uses a 1,024-bit or higher key space ( $10^{308}$  combinations).

Decryption times with modern hardware vary from seconds for 64-bit encryption to days or weeks for 512-bit encryption. Encryption algorithms using 1,024-bit or larger key spaces have yet to be cracked with commonly available hardware.