Glossary Words

Character
A letter, figure, punctuation mark, or other symbol used in writing or printing.

Cipher
A method or system of changing text to hide its real meaning where each letter is changed to something else.
For example: **A=D or A=# or A=._**

Cipher Alphabet
A table that shows what each letter is replaced with.
For example: **A=Z, B=Y, C=X, etc.**

Code
A system of changing entire words or phrases into something else.
For example: **President = Eagle, Battleship=13425.**

Codebook
A book or other document that lists the answers (the key) to the secret code.

Codebreaker
A person who uses cryptanalysis to solve secret codes and ciphers without having the key.

Codemaker
A person who makes new secret codes and ciphers.

Comint
Communications Intelligence, technical and intelligence information gathered from foreign communications by other than the intended recipients.

Crib
A method of codebreaking that uses part of the assumed (guessed) plain text to compare against the cipher.

Cryptanalysis
The part of cryptology that deals with studying a secret message or a group of secret messages and breaking the system so you can read what it says without first knowing the key.

Cryptogram
A message that has been written in a secret cipher.

Cryptography
The part of cryptology that deals with making codes or cipher systems so that others cannot read what is in the secret message.

Cryptologist
A person who makes and/or breaks codes.

Cryptology
The art and science of making (cryptography) and breaking (cryptanalysis) codes.

Cryptosystem
A method or process for changing regular text to hide its real meaning.

Decipher, Decode, Decrypt
To change a secret encoded message back to the real text so you can read it.

Encipher, Encode, Encrypt
To use a secret system to change a message into a secret message that only you and your friends who know how to read.

Enigma
Name for machine used by the Germans to encrypt and decrypt secret messages in World War II.

Information Assurance (IA)
This, the codemaking half of cryptology, is one of NSA's main missions.

Intelligence
Information about an enemy that has been studied for its importance and accuracy, and provided to warfighters and decision makers.

Jade
Codename for machine used by the Japanese Imperial Navy to encrypt and decrypt messages during World War II.

Key
A symbol or group of symbols used for controlling the making **(cryptography)** and breaking **(cryptanalysis)** of codes. For example, if your key is **A=B, B=C, C=D, etc.,** both you and your friend need to know that to encrypt and decrypt the message.

Plain Text
A message written in regular characters readable by all without any hidden or secret meaning.

Purple
Codename for the Japanese system of encrypting diplomatic messages during World War II.

Recovery
The process of figuring out a code or key by studying (cryptanalysis) the message or messages.

Service Cryptologic Elements (SCE)
Branches of the armed services that are members of the Intelligence Community:
* U.S. Naval Security Group
* U.S. Army Intelligence Security Command
* U.S. Air Force Air Intelligence Agency
* U.S. Marine Corps
* U.S. Coast Guard

Setting
The position of parts of a cryptosystem or cipher machine, like a starting point. For example, the Germans needed to set the ENIGMA machine to the right rotor setting before beginning to encrypt or decrypt their messages during World War II.

Sigint
Signals Intelligence, information gathered from the foreign signals environment that enables our government to make important decisions. This, the codebreaking half of cryptology, is one of the main missions of NSA/CSS. The protection of the rights of U.S. citizens is guaranteed by the 4th amendment to the Constitution.

Slide
The number of position changes between the plaintext and the encoded text.

if the plaintext is	**ABCDEFGHIJKLMNOPQRSTUVWXYZ**
and the enciphered text is	**VWXYZABCDEFGHIJKLMNOPQRSTU**
then the slide = 5.	12345

Substitution Cipher
A method of encrypting a message where the characters of the plaintext are in the same order but are switched to other characters, like **A=D, B=E, C=F, etc.**

Transposition Cipher
A method of encrypting a message where the character positions are changed but the characters themselves stay the same, like **SECRET=ECTRES.**