



# Cyber Security Initiative for Nevada Teachers (CSINT)

Brian La Torre, Dr. Shamik Sengupta, Dr. David Feil-Seifer, Dr. Nancy LaTourette, Steven Fisher, Tim Muller

## Implementing Cyber Security & Digital Forensics Into the Classroom

### Introduction & Justification

The purpose of this lesson is to introduce students to computer science principles that are associated with cybersecurity, and in particular, digital forensics. As technology becomes a more integral part of our daily lives, it is important to develop an understanding for how technological resources work. Students, for the most part, are unaware of security, protection and privacy issues while they are using computers, especially their mobile devices. Hashing is a computational calculation in which all files are given a mathematical value based on their unique contents. The significance of hashing, as related to digital forensics, verifies and authenticates sources of information. Cryptography includes techniques used to keep information private, secure and protected from interception. Two of the most common and well-known ciphers are the Pig Pen and Caesar ciphers. The introduction of these cipher examples will allow students to identify strategies to keep their information secure from threats and develop their own methods and algorithms for using cryptography as a part of their daily lives.

### Objectives & Standards

**Objectives:**  
Students will be able to:

- Understand the roles and functions of hashing
- Collect artifacts, in the form of images and other files, and identify them based on their hash values
- Learn the basic function of cryptography and complete activities based on the Pig Pen and Caesar ciphers
- Use cryptography to encrypt and decrypt messages

**Standards:**

**Computer Technology – Research and Information Fluency – Students apply digital tools to gather, evaluate and use information**

- 3.A.2.1 – Determine steps to answer a question using digital tools
- 3.C.a.2 – Select and justify appropriate digital resources to accomplish a variety of tasks

**CCSS ELA-Literacy.SL.11-12.2**

Integrate multiple sources of information presented in diverse formats and media in order to make informed decisions and solve problems, evaluating the credibility and accuracy of each source and noting any discrepancies among the data

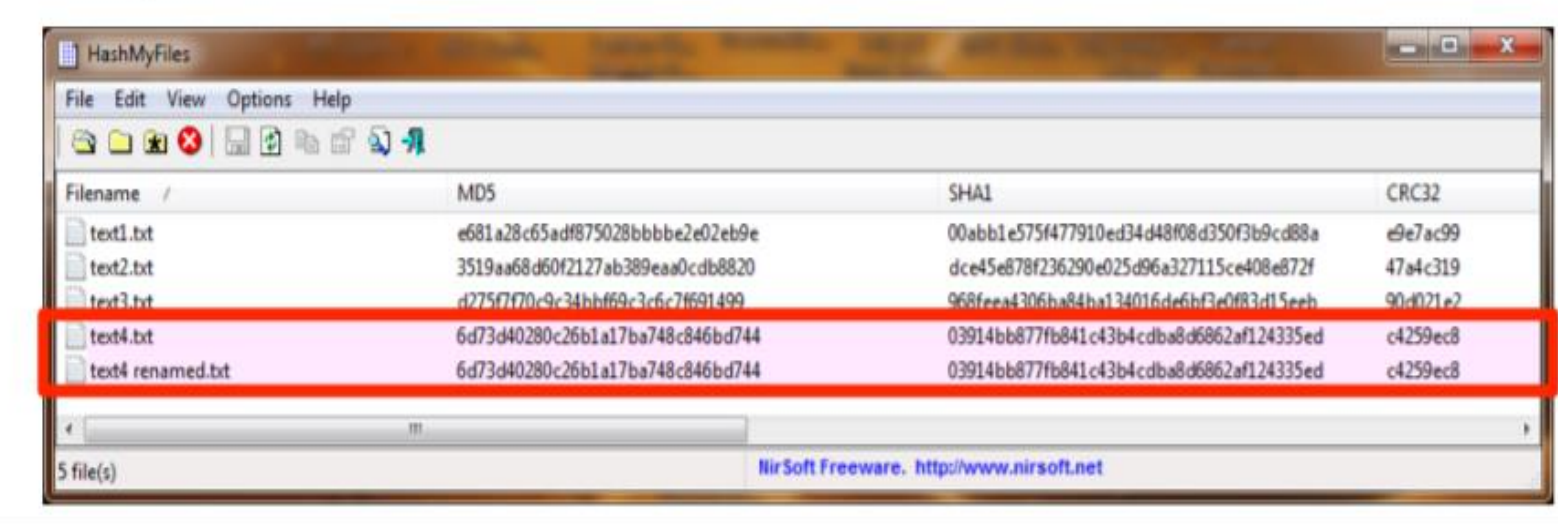


**Nevada Computer and Technology Standards**  
Classroom Technology Integration for the 21<sup>st</sup> Century

## Hashing

### HASHED messages in Text Files

File Name	Contents
text1.txt	"the quick brown fox jumped over the lazy dogs back"
text2.txt	"THE QUICK BROWN FOX JUMPED OVER THE LAZY DOGS BACK" (typed in all caps)
text3.txt	"the quick brown fox jumped over the lazy dogs back" (spaces added at end of sentence)
text4.txt	"The quick brown fox jumped over the lazy dogs back" (first letter of the first word in upper case)
test4 renamed.txt	"The quick brown fox jumped over the lazy dogs back" File renamed and saved text4.txt to test4 renamed.txt

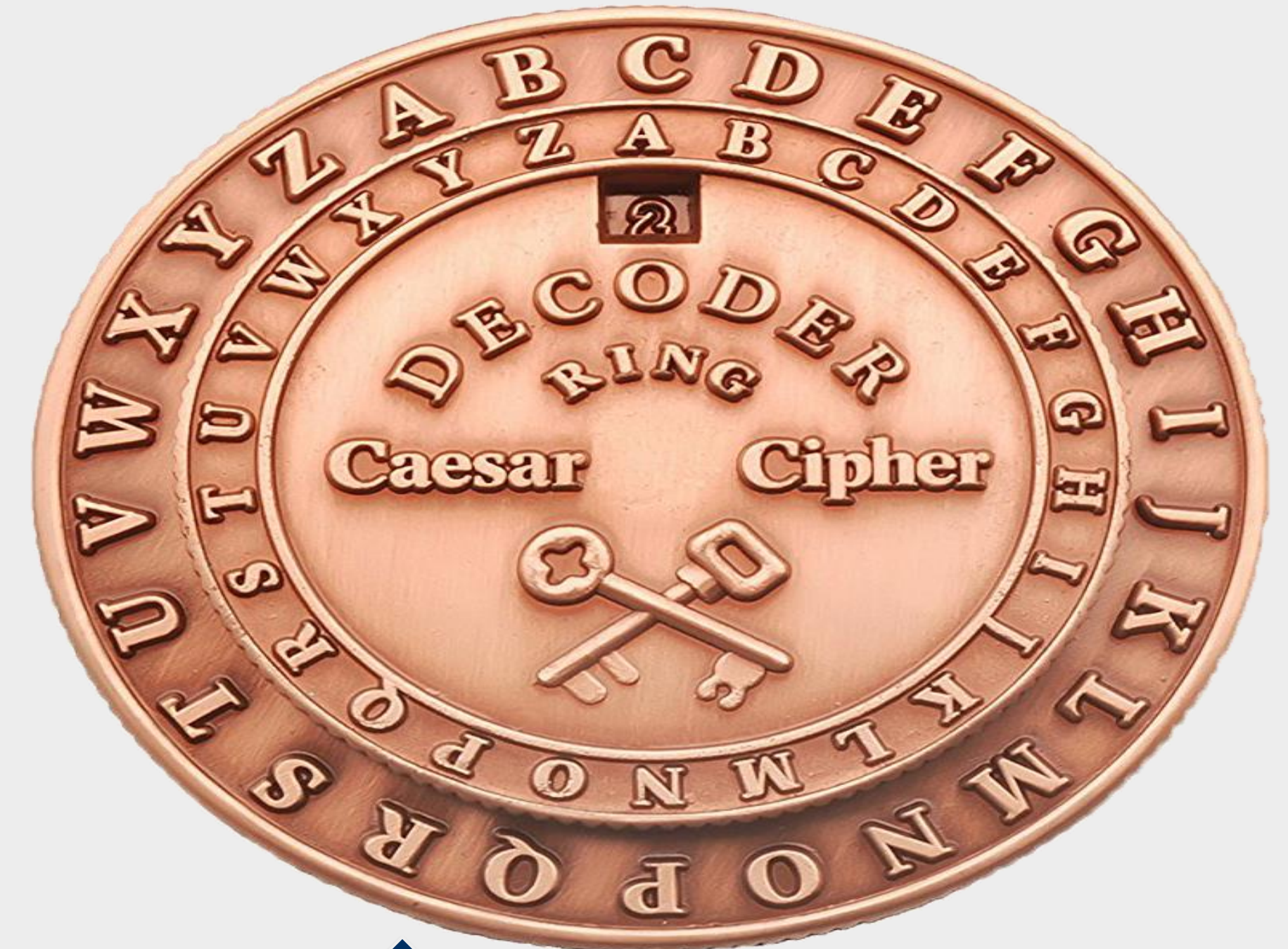


## Cryptography

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	.	.
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	00	0
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	.	.

Student #1	4 15 24 1 18 24 17 2 00 - graduate
Student #2	5 6 4 5 00 - high
Student #3	12 13 13 12 15 17 18 11 6 17 6 2 16 0 - opportunities
Student #4	16 13 24 18 8 16 00 - Sparks
Student #5	24 11 1 00 26 24 15 2 2 15 00 - and career
Student #6	10 6 16 16 6 12 11 00 - mission
Student #7	24 00 3 18 9 9 00 - a full
Student #8	16 26 5 12 12 9 00 - school
Student #9	2 1 18 26 24 17 6 12 11 24 9 00 - educational
Student #10	13 15 2 13 24 15 2 1 00 17 12 00 - prepared to
Student #11	16 17 18 1 2 11 17 16 00 - students
Student #12	24 26 26 2 16 16 00 - access
Student #13	20 6 9 9 00 - will
Student #14	15 24 11 4 2 00 12 3 00 - range of
Student #15	16 17 24 17 2 10 2 11 17 00 - statement
Student #16	24 16 00 13 15 12 1 18 26 17 6 19 2 - as productive
Student #17	13 12 16 17 00 16 2 26 12 11 24 15 22 00 - post secondary
Student #18	26 6 17 6 23 2 11 16 00 - citizens

## Engage



Caesar Cipher



Pig Pen Cipher

## Explore



Hashing is a mathematical calculation that is used as an identification of images and other types of files. The common hash functions are MD-5, SHA-1 and SHA-256. The MD-5 has become vulnerable and therefore not used as much. The SHA-1 hash (Secure Hash Algorithm) was developed by the United States government but has been dropped from the standards as the SHA-256 is now used primarily by the NSA. (National Security Agency)

## Elaborate

Cryptographic hash functions, like the example provided below, are used for verification and authentication purposes throughout modern cryptography. Ensuring the integrity of information is the primary purpose for developing hash functions.

Input	Digest
Fox	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps over the blue dog	8FD8 7558 7851 4F32 D166 76B1 79A9 0DA4 AEEF 4819
The red fox jumps over the blue dog	FC03 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps over the blue dog	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 32B9 6A6C

## Explain

16 13 24 18 8 16 00 5 6 4 5 00 16 26 5 12 12 9 00 10 6 16 16 6 12 11 00 16 17 24 17 2 10 2 11 17 00 16 17 18 1 2 11 17 16 00 20 6 9 9 00  
Sparks-High-School-Mission-Statement-Students-will-  
4 15 24 1 18 24 17 2 00 24 16 00 13 15 12 1 18 26 17 6 19 2 00 26 6 17 6 23 2 11 16 00 13 15 2 13 24 15 2 1 00 17 12 00 24 26 26 2 2 16 16 00  
Graduate-as-productive-citizens-prepared-to-access-  
24 00 3 18 9 9 00 15 24 11 4 2 00 12 3 00 13 12 16 17 00 16 2 26 12 11 1 24 15 22 00 2 1 18 26 24 17 6 12 11 24 9 00 24 11 00 26 24 15 2 2 15 00  
A-full-range-of-post-secondary-educational-and-career-  
12 13 13 12 15 17 18 11 6 17 6 2 16 0  
Opportunities!

Cryptography is the art of writing and solving codes. Students will learn the Pig Pen and Caesar ciphers before developing their own strategies and ciphers to protect information. The above image breaks down our school's mission statement but is based on a numerical version of the Caesar cipher, which was developed centuries ago by Julius Caesar to protect significant military information. Students will learn to encrypt their messages and decrypt messages like the example above.

## Evaluate

