Lab - Exploring Encryption Methods

Objectives

Part 1: Decipher a Pre-Encrypted Message Using the Vigenère Cipher

- Use an encrypted message, a cipher key, and the Vigenère cipher square to decipher the message.

Part 2: Create a Vigenère Cipher Encrypted Message and Decrypt It

- Work with a lab partner and agree on a secret password.
- Create a secret message using the Vigenère cipher and the key.
- Exchange messages and decipher them using the pre-shared key.
- Use an interactive Vigenère decoding tool to verify decryption.

Background

The Cisco IOS password encryption service uses a Cisco-proprietary algorithm that is based on the Vigenère cipher. Vigenère is an example of a common type of cipher mechanism called polyalphabetic substitution.

Note: Students can work in teams of two for this lab.

Required Resources

Device with internet access

Instructions

Part 1: Decipher a Pre-Encrypted Message Using the Vigenère Cipher

In Part 1, you will analyze an encrypted message and decrypt it using a cipher key and the Vigenère cipher square.

Step 1: Review the encrypted message.

The following message has been encrypted using the Vigenère cipher:

GGIATVWGQIR

Step 2: Review the cipher keyword.

The cipher keyword **TCPIP** was used to encrypt the message. The same keyword will be used to decrypt or decipher the message.

Step 3: Review the structure of the Vigenère square.

A standard Vigenère square or table is used with the keyword to decipher the message.

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

Step 4: Decrypt the message using the keyword and Vigenère square.

a. Use the table below to help you decrypt the message. Start by entering the letters of the encrypted message in the second row of cells, from left to right.

b. Enter the keyword TCPIP in the top row, repeating the letters until there is a keyword letter for each letter of the encrypted message, even if the keyword letters at the end do not represent the complete keyword.

c. Refer to the Vigenère square or table shown in Step 3 and find the horizontal row that starts with the first letter of the keyword (the letter T). Scan across that row and locate the first letter of the encrypted message in the row (the letter G). The letter at the top of the column where the encrypted message letter appears is the first letter of the decrypted message (the letter N).

d. Continue this process until you have decrypted the entire message and enter it in row 3 of the following table.

Cipher Keyword											
Encrypted Message											
Decrypted Message											

Part 2: Create a Vigenère Cipher-Encrypted Message and Decrypt It

In Part 2, work with a lab partner and agree on a secret password to use as the pre-shared key. Each lab partner creates a secret message using the Vigenère cipher and the key. Partners exchange messages and decipher them using their pre-shared key.

Note: If you do not have a partner, you can perform the steps yourself.

Step 1: Determine the cipher keyword.

With your partner, establish a cipher keyword and enter it here.

Step 2: Create a plain text message and encrypt it (both partners).

a. Create a plain text (decrypted) message to be encrypted by your partner.

Record it below.

b. You can use the following table to help you encrypt the message. You can enter the unencrypted message and cipher keyword here, but do not let your partner see it.

c. In the Vigenère table, locate the row that starts with the first letter of the cipher keyword. Next locate the first letter to be encrypted at the top of the column in the table. The point (cell) at which the table row (key letter) and column (message letter) intersect is the first letter of the encrypted message. Continue this process until you have encrypted the entire message.

Note: This table is limited to messages of 12 characters. You can create longer messages if desired. Message encryption and decryption are not case-sensitive.

Cipher Keyword												
Encrypted Message												
Decrypted Message												

Step 3: Decrypt the message from your partner.

a. You can use the following table to help you decrypt your partner's encrypted message. Enter the encrypted message from your partner and the cipher keyword.

b. Use the same procedure described in Part 1, Step 4.

Note: This table is limited to messages of 12 characters. You can create longer messages if desired.

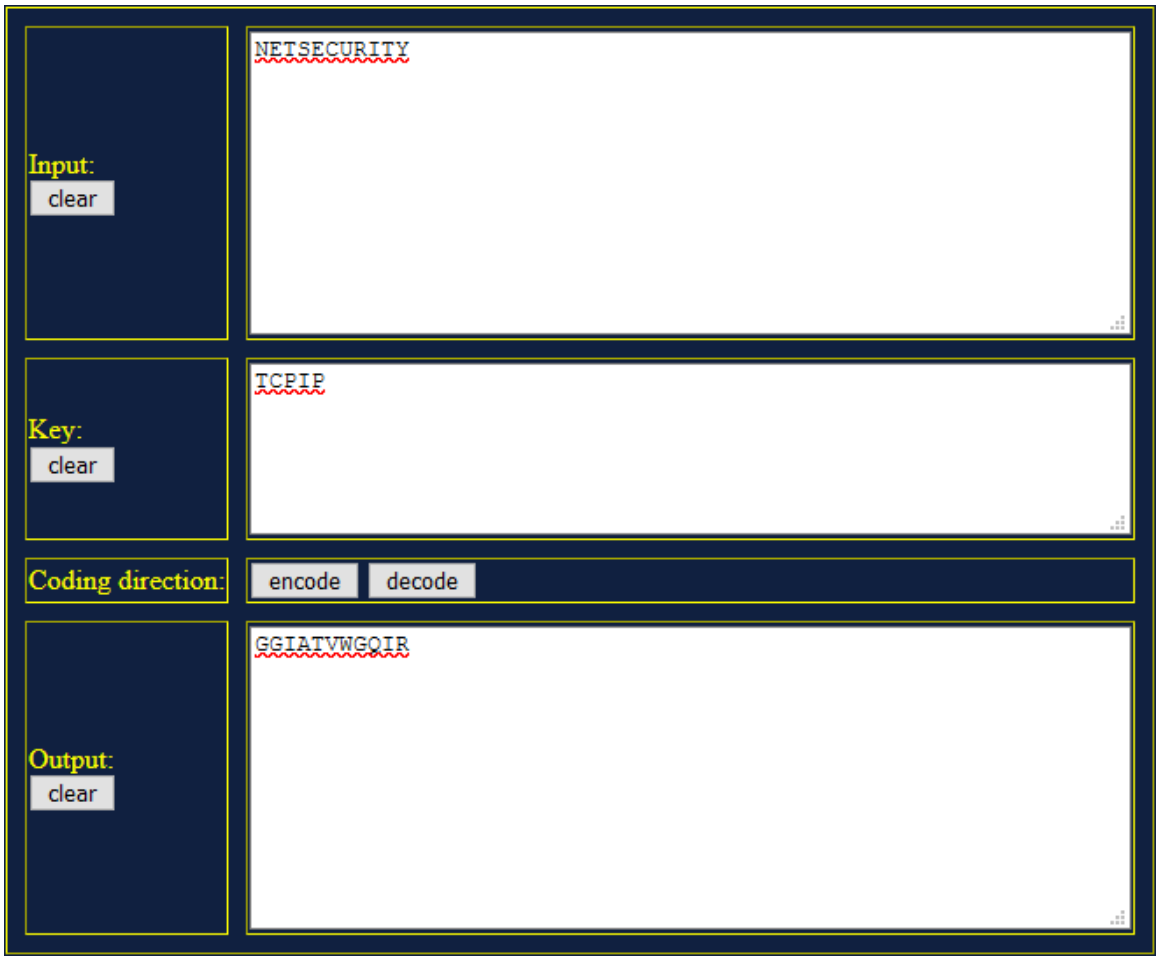
Cipher Keyword												
Encrypted Message												
Decrypted Message												

Step 4: Use an interactive decryption tool to confirm decryption.

a. An internet search for "Vigenère decode" shows that various cipher encryption and decryption tools are available. Many of these are interactive.

b. One interactive tool is located at http://sharkysoft.com/vigenere/1.0/. At this site, enter the encrypted message from your partner in the top part of the screen and the cipher key in the middle. Click **Decode** to see the clear text version of the message. You can also use this tool to encrypt messages.

c. The following example uses Sharky's Vigenère Cipher tool to decode the encrypted message from Part 1.



Reflection

1. Could the Vigenère cipher be used to decode messages in the field without a computer?

2. Search the internet for Vigenère cipher cracking tools. Is the Vigenère cipher considered a strong encryption system that is difficult to crack?