My name is _____

The CyBears Need Your Help!

Can you unscramble the words below to help decipher what Grace CyBear can do to keep her electronic devices safe from bad guys?

1. NTUARVSII   _____

2. AILFLWRE   _____

3. ECNONPRITY   _____

4. OTPEYHON   _____

5. ASRPOWDS   _____

6. SROTAEFW UDEPTA   _____

Great job! Now, Alan CyBear needs cyber sleuths like you to help him understand some of the words you just unscrambled. Use the context to find the answers!

7. When logging into an electronic device, you use this **secret word** to gain access to the system.
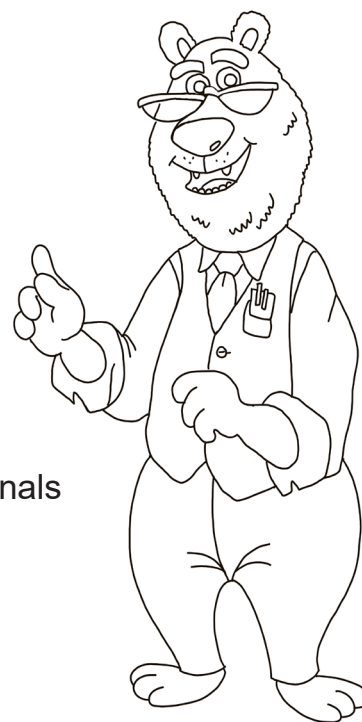
     a. Firewall   b. Password   c. Encryption

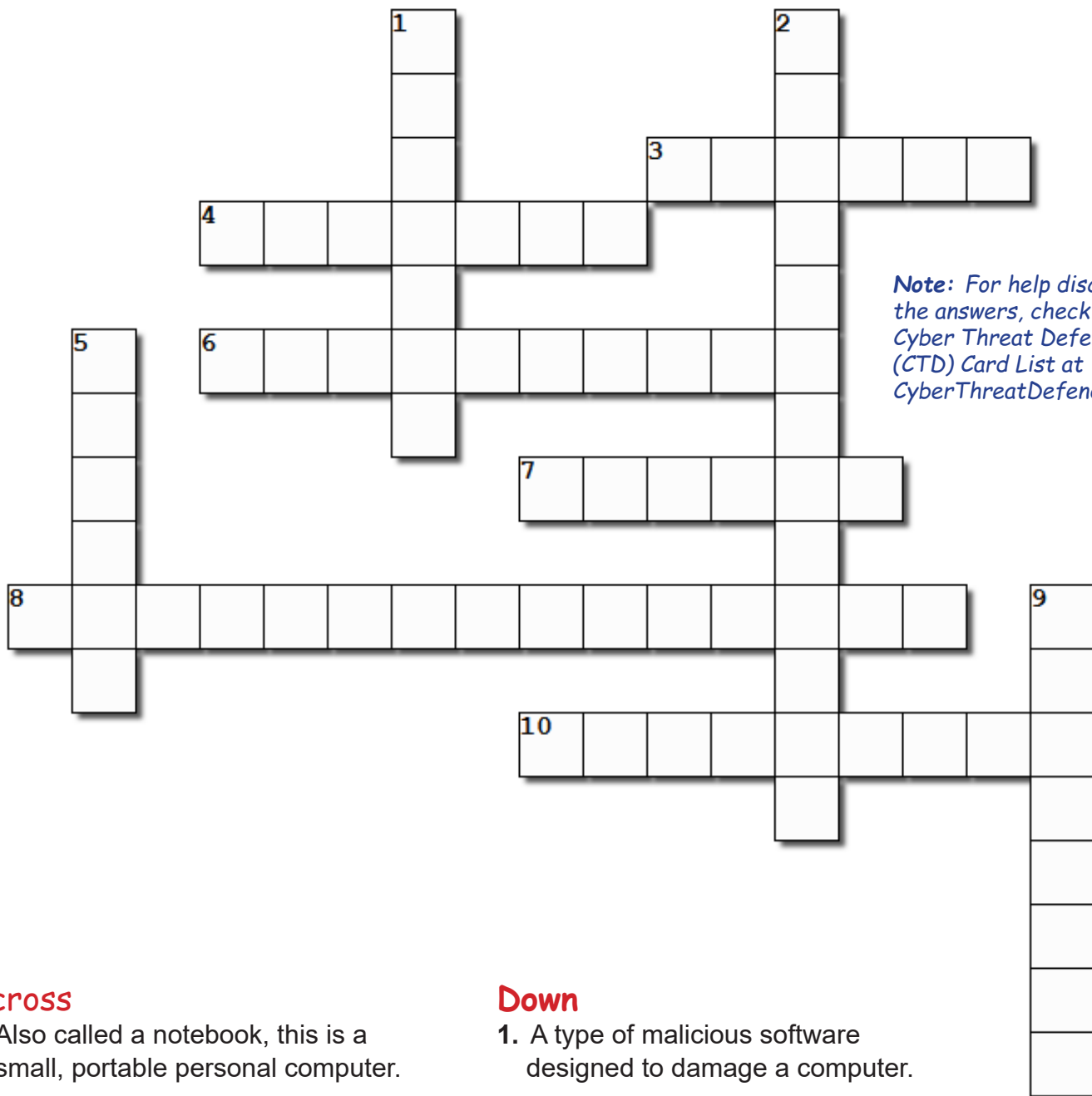8. Part of a computer system that is designed to **block** unauthorized access to important information.

     a. Anti-Virus   b. Honeypot   c. Firewall

9. This is a decoy used to **attract** cyber attackers and capture them **sticky**-"handed" in a crime. This trap helps cybersecurity professionals to detect and learn more about the attacker's activities and prevent future cyber crimes.

     a. Update Software   b. Anti-Virus   c. Honeypot

Note: *For help discovering the answers, check out the Cyber Threat Defender (CTD) Card List at CyberThreatDefender.com*

Across

3. Also called a notebook, this is a small, portable personal computer.

4. Type of malware that secretly sends information about your data to an attacker.

6. Process of encoding a message that only certain people can access.

7. A device that provides access to the Internet.

8. A personal computer designed for regular use at a single location.

10. Type of malware that reports all your actions online to an attacker.

Down

1. A type of malicious software designed to damage a computer.

2. This establishes a connection between your computer and the Internet.

5. This system is more powerful, has more memory, and is dedicated to running your network services.

9. A network security system that monitors and controls information coming in and out of a network.

Matching Online Terms

Ada CyBear is helping explain common definitions for using the Internet and connecting with friends online to her grandmother. However, Ada is also getting confused. Help Ada and her grandmother match the correct word with their definition.

Circle the correct answer below. *HINT: Review the Pronoun sentences on page 8 for clues to the answers.*

1 Rules or manners for interacting courteously with others online.

A) Etiquette   C) Setiquette

B) Detiquette   D) Netiquette

2 A list of friends a user interacts with online through various media, such as instant messaging (IM) and chat.

A) Yearbook   C) Buddy List

B) Cloud   D) Skywalkers

3 Methods individuals use to track, lure, or harass another person online.

A) Spyware   C) Spam

B) Cyberstalking D) Cipher

4 A location online that allows multiple users to communicate electronically with each other in real time.

A) Chatroom   C) Social Room

B) Modem   D) Browser

5 Willful and repeated harm inflicted through electronic text, typically through emails or websites.

A) Cyberbullying C) Botnet

B) Grey Hat   D) Flame

6 The nickname a user has chosen to be identified by when playing Internet games.

A) Cybercop   C) User

B) Droid   D) Gamer Tag

7 A diary or personal journal kept on a website, usually updated frequently, and are grouped by specific subjects.

A) Real-time   C) Banner

B) Blog   D) Post

8 Internet gamers who intentionally cause problems or cyberbully other gamers.

A) Vaders   C) Black Hatters

B) Blended Threat D) Griefers

Cybersecurity for All Crossword Puzzle
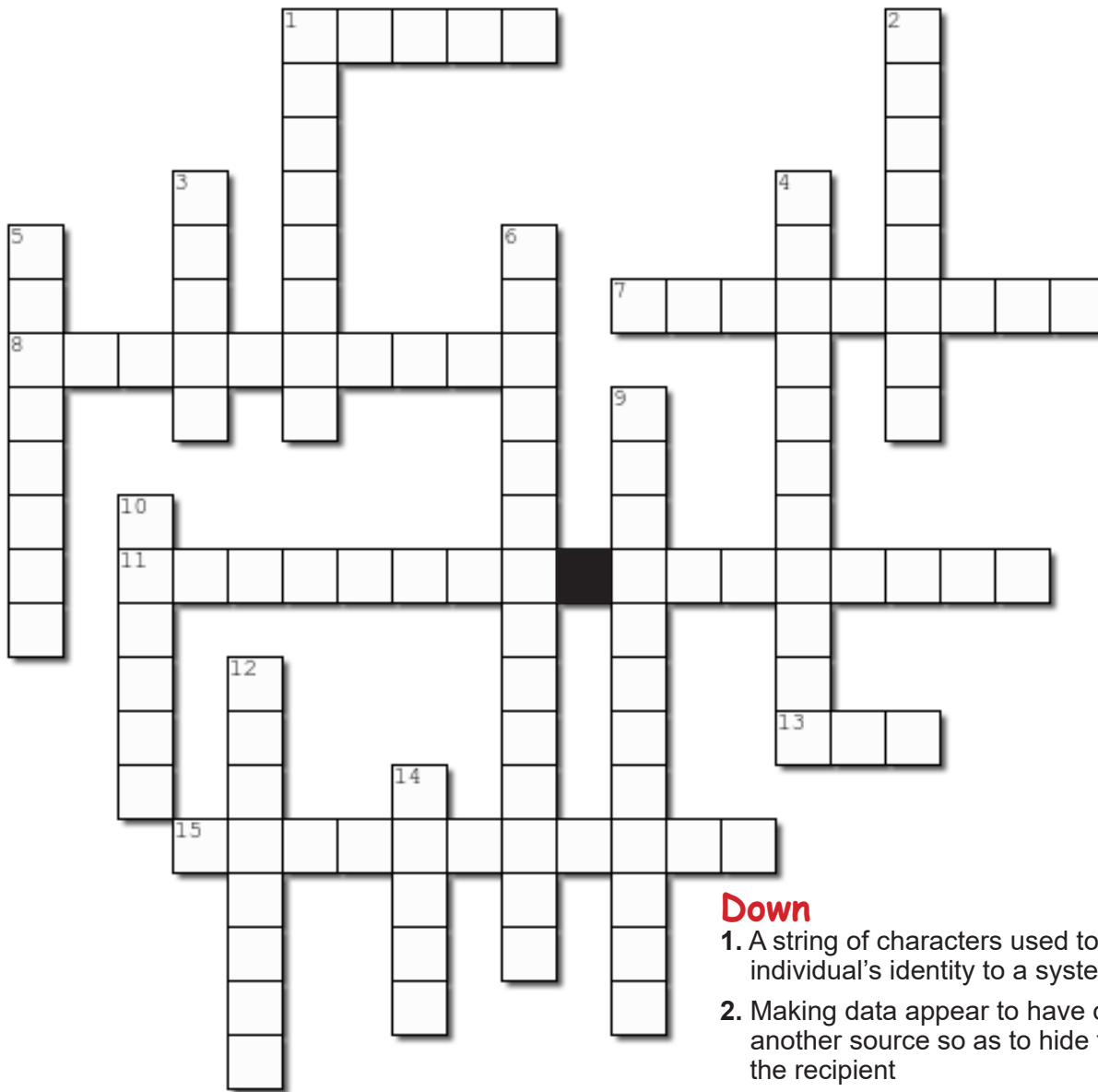
Across

1. A replacement set of code designed to correct problems or weaknesses in existing software

7. A step-by-step procedure used to solve a problem

8. Used to show the result of an encryption algorithm

11. The network layer protocol used by the Internet for routing packets across a network

13. A sequence of characters or bits used by an algorithm to encrypt or decrypt a message

15. A cryptographically signed object that contains an identity and a public key associated with this identity

Down

1. A string of characters used to prove an individual's identity to a system or object

2. Making data appear to have originated from another source so as to hide the true origin from the recipient

3. The temporary storage of information before use, typically used to speed up systems

4. A type of attack that overwhelms a server or network with more traffic than it can handle, resulting in the system crashing

5. A hidden method used to gain access to a computer system, network, or hidden application

6. The process by which a subject's (or a user's) identify if verified

9. The art of secret writing that enables someone to hide the contents of a message or file from everyone but the person received

10. A coding system that converts messages into ciphertext using its algorithm and key

12. A network device used to segregate traffic based on rules

14. A form of malware or software that attaches itself to other pieces of code in order to replicate

Read each definition and circle the word that is spelled correctly.

1. Method to protect the privacy of information by encrypting it into a secret code.

   Cryptography   Cryptographie   Criptegraphy

2. Processes employed to safeguard and secure crucial information of an organization.

   Cibersecurity   Cybearsecurity   Cybersecurity

3. Malicious intent to prevent the users of the cryptosystem from achieving their goal.

   Advirsary   Adversary   Advesary

4. Process of monitoring and recording data that is flowing between two points in a communication system.

   Wiretaping   Waretapping   Wiretapping

5. An algorithm for performing encryption or decryption of code.

   Ciypher   Cipher   Cepher

6. Process of decoding cipher text to plain text, so it is readable by the user.

   Dicryption   Decription   Decryption

7. A secret sequence of characters that is used as a form of authentication to confirm a user's identity in a computer program or online.

   Passwerd   Password   Pasword

8. An expert programmer who uses computer systems to gain unauthorized access to a computer system.

   Hacker   Haker   Hakcer

9. An action to deliberately change or alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

   Taemper   Tamper   Tampper

10. A flaw that allows someone to operate a computer system with authorization levels in excess of that which the system owner specifically granted.

    Valnerability   Vulneriblity   Vulnerability

Caesar Cipher

The Roman Emperor Gaius Julius Caesar used the shift cipher, also known as the Caesar Cipher, to encrypt messages he sent to his generals. To encrypt a word or message means to hide that message by turning it into a secret code. If you'd like to send secret messages to your friends or family, the shift cipher may be the way to go!

A **shift cipher** is a type of substitution cipher that works by shifting the ciphertext from their original position to a new position in the alphabet. The plaintext is replaced with ciphertext that is in that position.

To begin the exercise, look at the two rows of the alphabet below. The top row is in plaintext (PT) and the bottom row will be your ciphertext (CT).

PT	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
CT	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

The table above shows the ciphertext row has shifted by three positions to the left.

In a shift cipher, the key is the number of spaces a ciphertext has shifted and it is what is used to encrypt or decrypt messages. Remember, in this example the chosen "key" is three (3). Now, let's move on to encryption and decryption!

Encryption & Decryption

To encrypt a word, you'll need to look at the plaintext first and figure out what it will become by looking at the letter below it. Using the table above, notice that the letter, or plaintext, *"A" will become "D" in ciphertext.* Use the cipher key (the table above) to encrypt the following words:

Password - ___ ___ ___ ___ ___ ___ ___ ___

Encryption - ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Great Job! Now try decryption to change an encrypted word back into plaintext. This time you'll need to look at the ciphertext first (bottom row) and see what it will be in plaintext. *The ciphertext "B" is actually "Y" in plaintext.*

GHFUBSW - ___ ___ ___ ___ ___ ___ ___

Shift Cipher - Decoding

Let's practice using the oldest type of cipher, the Caesar Cipher! Also known as a shift cipher, Alan CyBear needs your help filling in the ciphertext (CT) row below by using a key of 3. This means you will needs to shift the alphabet by three positions. The first letter has been done for you.

Remember, the first row is the plaintext (PT), and the CT row is used to help you encode and decode a message.

PT	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
CT	D

For each sentence below, decipher the messages using the shift cipher key of 3 above. For example, "L ORYH FKHHVH" becomes "I LOVE CHEESE".

1. QHYHU JLYH RXW SHUVRQDO LQIRUPDWLRQ.

_____

2. FUHDWH XQLTXH SDVVZRUGV.

_____

3. WKLQN WZLFH EHIRUH BRX SRVW.

_____

4. WKLQN WZLFH EHIRUH BRX FOLFN.

_____

5. VSHDN XS GRQ'W VWDQG IRU EXOOBLQJ.

_____

Caesar Cipher - Encoding

Let's practice using the oldest type of cipher, the Caesar Cipher! Also known as a shift cipher, Grace CyBear needs your help filling in the ciphertext (CT) row below by using a key of 3. This means you will needs to shift the alphabet by three positions. Fill in the CT row to encrypt the messages below.

Remember, the first row is the plaintext (PT), and the CT row is used to help you encode and decode a message.

PT	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
CT																										

For each sentence below, encipher the messages using the shift cipher key of 3 above. For example, "I LOVE CHEESE" becomes "L ORYH FKHHVH".

1. Keep your passwords secret.

_____

2. Be respectful when you are online.

_____

3. Do not talk to strangers.

_____

4. Tell an adult when you feel threatened or scared.

_____

5. Ask before you download.

_____

Shift Cipher - Decoding Secret Messages

Keep practicing the shift cipher by decoding the secret messages below. Start by filling in the ciphertext (CT) with a shift key of 5. Next, decode the messages.

Code: Shift Cipher
Key: Shift + 5

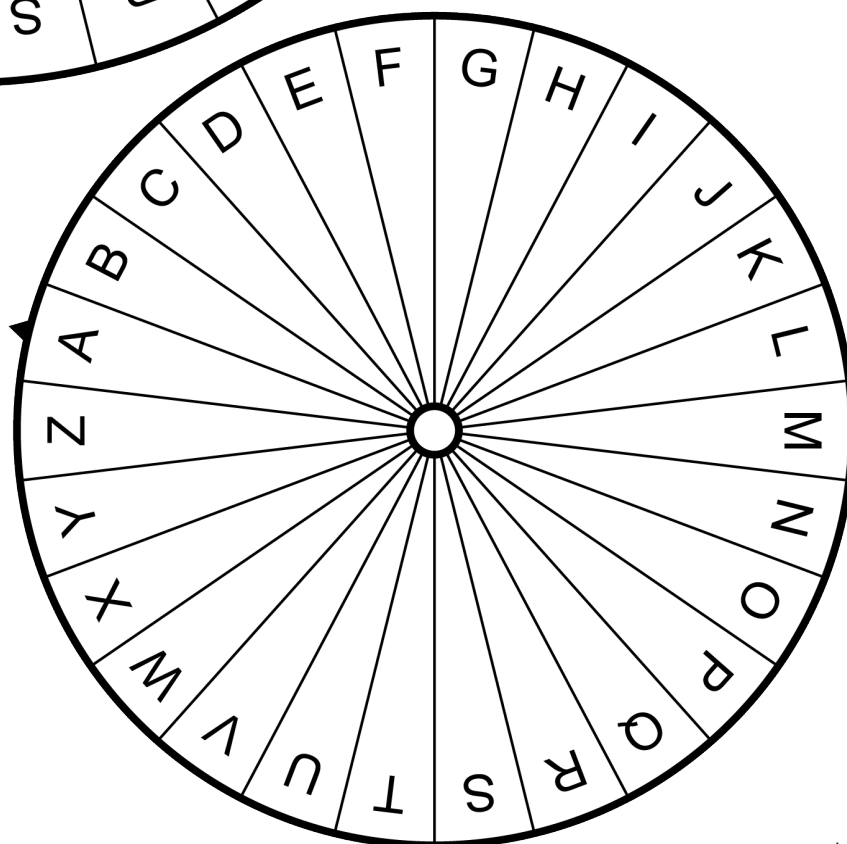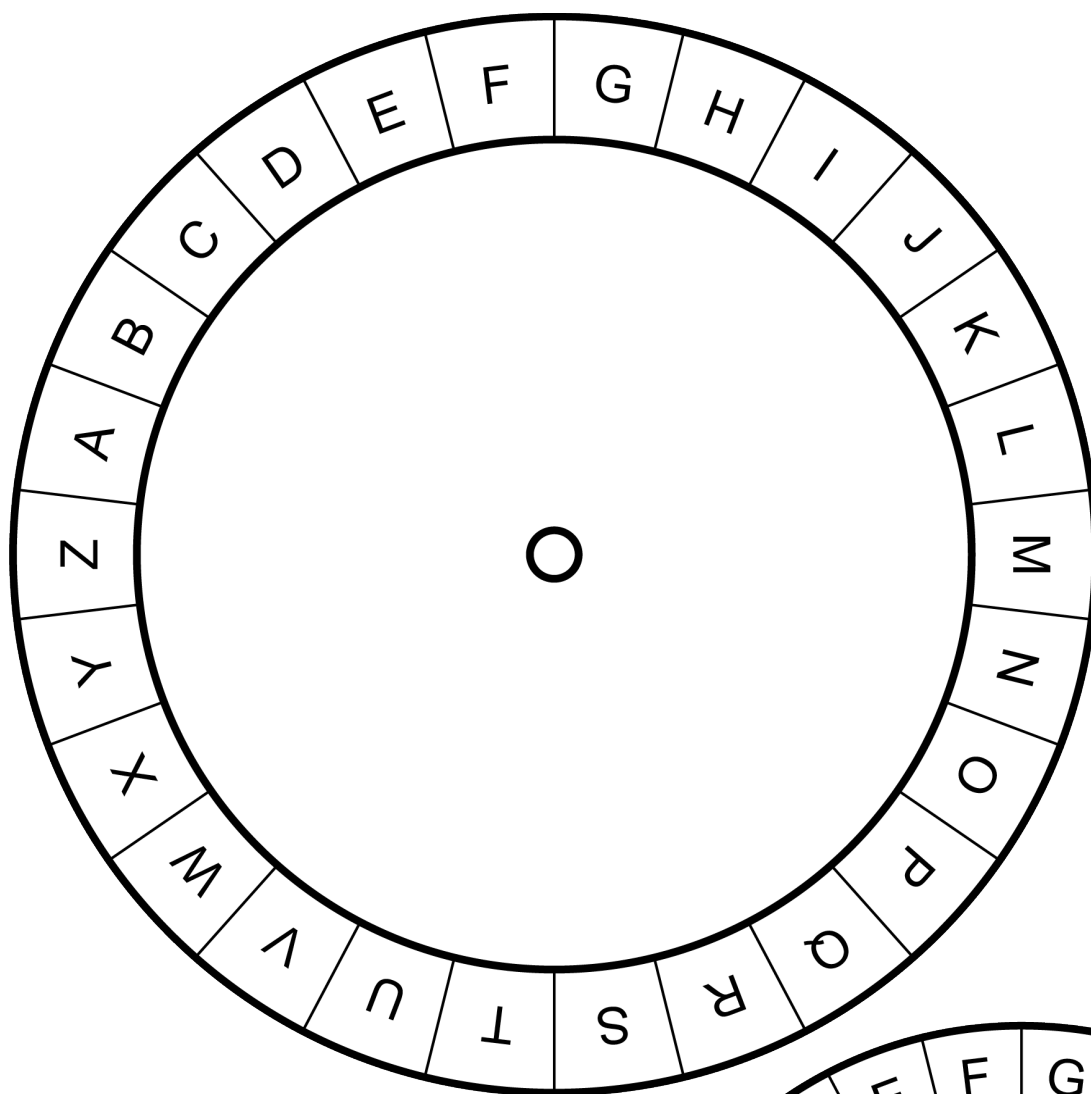| PT	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
CT	

Coded Message 1:

V YZIDVG JA NZMQDXZ VOOVXF XVI KMZQZIO
V XJHKPOZM AMJH VXXZNNDIB RZWNDOZN

_____

_____

_____

_____

Coded Message 2:

RDMZGZNN MJPOZMN VGGJR YZQDXZN GDFZ
KCJIZN OJ XJIIZXO OJ OCZ DIOZMIZO

_____

_____

_____

_____

Cipher Wheel - Encryption

The **cipher wheel** is a tool used to encrypt and decrypt shift ciphers using a "key".

The large wheel is your **plaintext** and the smaller wheel is your **ciphertext**. To use wheels, cut out both wheels on page 24 and place the smaller wheel on top of the large wheel.

Now that you have your cipher wheel, **shift the ciphertext around to the left** to solve puzzles with more than one key. Try encrypting the following phrases using your cipher wheel.

The number below each word is the unique key for that word.

Message 1:

CYBERSECURITY   IS   A   SHARED   RESPONSIBILITY
5   3   14   9   22

_____ ____ __

_____ _____

Message 2:

CRYPTOGRAPHY   CAN   CREATE   SECRET   MESSAGES
9   1   13   7   18

_____ _____

_____ _____ _____

Message 3:

BREAK   THE   CODE   USING   A   CIPHER   WHEEL
23   8   11   5   2   25   4

_____ ____ ____ _____

__ _____ _____

PAGE 1
1. Antivirus
2. Firewall
3. Encryption
4. Honeypot
5. Password
6. Software Update
7. b
8. c
9. c

PAGE 2
1. malware
2. ISPConnection
3. laptop
4. spyware
5. server
6. encryption
7. router
8. desktopcomputer
9. firewall
10. keylogger

PAGE 3
1. D   2. C   3. B   4. A
5. A   6. D   7. B   8. D

PAGE 4
Across
1. patch
7. algorithm
8. ciphertext
11. internet protocol
13. key
15. certificate

Down
1. password
2. spoofing
3. cache
4. ddos attack
5. backdoor
6. authentication
9. cryptography
10. cipher
12. firewall
14. virus

PAGE 5
1. Cryptography
2. Cybersecurity
3. Adversary
4. Wiretapping
5. Cipher
6. Decryption
7. Password
8. Hacker
9. Tamper
10. Vulnerability

PAGE 6
Password - SDVVZRUG
Encryption - HQFUBSWLRQ
GHFUBSW - DECRYPT

PAGE 7
1. Qhyhu jlyh rxw shuvrqdo lqirupdwlrq =
Never give out personal information
2. Fuhdwh xqltxh sdvvzrugv =
Create unique passwords
3. Wklqn wzlfh ehiruh brx srvw =
Think twice before you post
4. Wklqn wzlfh ehiruh brx folfn =
Think twice before you click
5. Vshdn xs, grq'w vwdqg iru exooblqj =
Speak up, don't stand for bullying

PAGE 8
1. Keep your passwords secret =
Nhhs brxu sdvvzrugv vhfuhw
2. Be respectful when you are online =
Eh uhvshfwixo zkhq brx duh rqolqh
3. Do not talk to strangers =
Gr qrw wdon wr vwudqjhuv
4. Tell an adult when you feel threatened or scared
= Whoo dq dgxow zkhq brx ihho wkuhdwhqhg ru vfduhg
5. Ask before you download =
Dvn ehiruh brx grzqordg

PAGE 9
Coded Message 1: A DENIAL OF SERVICE ATTACK CAN PREVENT A COMPUTER FROM ACCESSING WEBSITES

Coded Message 2: WIRELESS ROUTERS ALLOW DEVICES LIKE PHONES TO CONNECT TO THE INTERNET

PAGE 11
Message 1:
CYBERSECURITY   IS   A   SHARED
HDGJWXJHZWNYD   LV   O   BQJANM

RESPONSIBILITY
NAOLKJOEXEHEPU

PAGE 11 (Continued)

Message 2:
CRYPTOGRAPHY   CAN   CREATE
HWDUYTLWFUMD   DBO   PERNGR

SECRET   MESSAGES
ZLJYLA   EWKKSYWK

Message 3:
BREAK   THE   CODE   USING   A
YOBXH   BPM   NZOP   ZXNSL C

CIPHER   WHEEL
BHOGDQ   A L I I P

Join the Fun & #DefendYourNetwork Today!   CIAS

Follow the CIAS: in f t