|  |  |  |
| --- | --- | --- |
|  | **Worksheet - Reading Guide for Keys and Passwords** |  |

# Keys and Passwords

## Your task

* Read [*Blown to Bits,* Chapter 5](http://www.bitsbook.com/wp-content/uploads/2008/12/chapter5.pdf), pp. 170-173:
  + **Start** right after the picture of the Vigenère cipher grid.
  + **Stop** at “Lessons for the Internet Age.”
* *With a partner,* answer the questions about the reading below.

**Questions:** Read the text and answer the following questions along with a partner

1. In cryptography, who are Alice, Bob and Eve?

Alice is the one sending the message. Bob is the one receiving the message. Eve is the one that is trying to intercept the message.

1. How is an encrypted message like a lock box?

The encrypted message has to have a certain key to be decrypted and read.

1. Yes or no: the Vigenère cipher is still used today in modern cryptography. Why or why not?

No because Charles Babaage recognized that if you had the length of the key then you could easily trial and error it or brute force it or even guess it.

1. What is “brute force decryption”?

Brute force decryption is trying every single possible key or solution for the encrypted message.

1. How long would a one-time pad need to be in order to encrypt a secret message that was 50 characters in length?

50 characters long

1. According to the reading, using modern cryptographic methods, if you increase the key length by 1 bit, how much more computation would be required to find (or “crack”) the key?

It would need to double the computation level to crack the key.

# Cryptographic Keys and Your Passwords

If you have ever joined a website where you had to create an account to login, you also had to create a password. That password is used as a key to do a variety of things at that site, but mostly it’s used to authenticate (prove) who you are.

When you created your password, the site may have presented you with some rules for your password, such as:

* must be at least 8 characters long
* must contain at least one number
* must contain at least one uppercase letter
* must contain at least one punctuation symbol (e.g. `-=[]\;’,./~!@#$%^&\*()\_+{}|:”<>?)

**Question:** Based on what you know about how keys work in cryptography, give a reason for why these rules require:

a) a certain number of characters

b) a mix of letters, numbers, uppercase and symbols

# Try It

## Caution! Can you trust this site?

In a separate tab or window:

* Go to: <https://howsecureismypassword.net/>
* Before you type anything: open the Developer Tools in your browser and make sure you can see any network traffic. This website lets you test the strength of various passwords. As the website tells you:

|  |
| --- |
| This site could be stealing your password... it's not, but it easily could be.  Be careful where you type your password. |

By opening the developer tools to inspect the traffic, you can make sure that’s true. In any event, if you want to be super careful, do not use any real password here.

## Test some passwords

For everything you try, make sure to:

* Click “show details.”
* Read the other statistics and facts about the password.

Try different passwords to see what the tool tells you:

* Try typing common words from the dictionary or well-known names like “apple” or “chicago”.
* Try typing something that’s over 16 characters.
* Try a string of 4 random words together, like AppleChicagoBalletTree.
* Type a 0. Then keep typing 0s and watch what happens to the statistics. (Actually, you might want to just hold 0 down for a while.)
* Try other things that interest you.

## Answer these questions

It’s very common for websites to require a password of at least 8 characters. Let’s explore how secure these passwords really are.

* Create a few passwords using 8 lowercase ASCII characters (a-z). What’s the longest amount of time-to-crack you can generate?

22 minutes

* Using any characters on the keyboard, what’s the longest amount of time-to-crack you can generate with an 8-character password?

22 minutes

* As you try passwords, what seems to be the single most significant factor in making a password difficult to crack? Why do you think this is?

The more differences between characters.

* Opinion: Is an 8-character minimum a good password length for websites to require? Give your opinion, yes or no, and explain why you think that.

No because if you make them longer then there are more places to make differences thus making it harder to solve.

* The AP CS Principles framework contains the following statement: Implementing cybersecurity has software, hardware, and human components. Based on what you’ve learned so far, describe at least one way that cybersecurity involves “human components.”

Cybersecurity is always at risk due to human components such as human error and intelligence to be interfering with the best security currently possible at the time. Human error can ruin any security in just a few seconds.

Hopefully you can now appreciate this comic: <http://xkcd.com/936/>

# CAPTCHA

[Click here](https://mass.pbslearningmedia.org/resource/nsn09.sci.engin.design.vonahn/luis-von-ahn-computer-scientist/#.WbnlIogrKCh)

Define/ explain CAPTCHA:

CAPTCHA is a test to figure out if it is a human or not. The secret password people can read but computers can’t.

What is RECAPTCHA and what are you doing when you solve one?

RECAPTCHA is two tests of CAPTCHA that include one test that the computer understands the answer to and one test that it doesn’t. The second test that the computer doesn’t know is most probably from an old book that they are trying to digitalize.