|  |  |  |
| --- | --- | --- |
|  | **Worksheet - Reading Guide for Encryption** |  |

## 

## Your Task

* Read two sections in [*Blown to Bits,* Chapter 5](http://www.bitsbook.com/wp-content/uploads/2008/12/chapter5.pdf), pp. 165-169:
  + **Historical Cryptography** (starts on p. 165)
  + **Breaking Substitution Ciphers** (starts on p. 166)
  + Don’t continue further.
* *With a partner,* answer the questions about the reading below.

## Vocabulary

* **Encryption** is the art of encoding messages so they can’t be understood by eavesdroppers or adversaries who might intercept them or spy.
* **Cryptography** is the field of study or practice of encryption and other techniques associated with sending secure communications.

**Questions**

Read the text and answer the following questions along with a partner.

1. How long has the art of cryptography been practiced?

About 4000 years

1. Encrypt this message using the Caesar Cipher, as shown on p. 165:

plaintext: CS IS COOL

ciphertext: FV LV FRRO

1. A Caesar Cipher is an example of a large class of ciphers known as substitution ciphers.
2. The section called *Breaking Substitution Ciphers* (p. 166) describes a “random substitution cipher,” in which each letter of the alphabet is randomly replaced with a different letter or character i.e. A→T, B→F… What makes a random substitution cipher more secure than a Caesar shift?

There is no real true pattern in a random substitution cipher compared to Caesar shift.

1. The reading shows a technique for cracking Chaucer’s text, which was encrypted using a basic substitution cipher. That technique, which takes advantage of the fact that certain characters or groups of characters occur more often than others and can be used to crack any substitution cipher, is called: frequency analysis.
2. Check the appropriate box:

According the reading, a random substitution cipher…

|  |  |  |
| --- | --- | --- |
|  | Is **actually** **easy**  to crack | Is **actually** **hard**  to crack |
| **Looks** **easy**  to crack |  |  |
| **Looks** **hard**  to crack | X |  |

1. **Make a prediction**

A Caesar shift cipher is supposedly easier to crack than random substitution. How long do you think it would take *you* to crack a message encrypted with a simple Caesar shift cipher? Note: there is no correct answer here; you’re just making a prediction. **Circle one.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Less than 1 minute | About 1 minute | 5 - 10 minutes | 10 - 20 minutes | More than 20 minutes |