Secure Communications

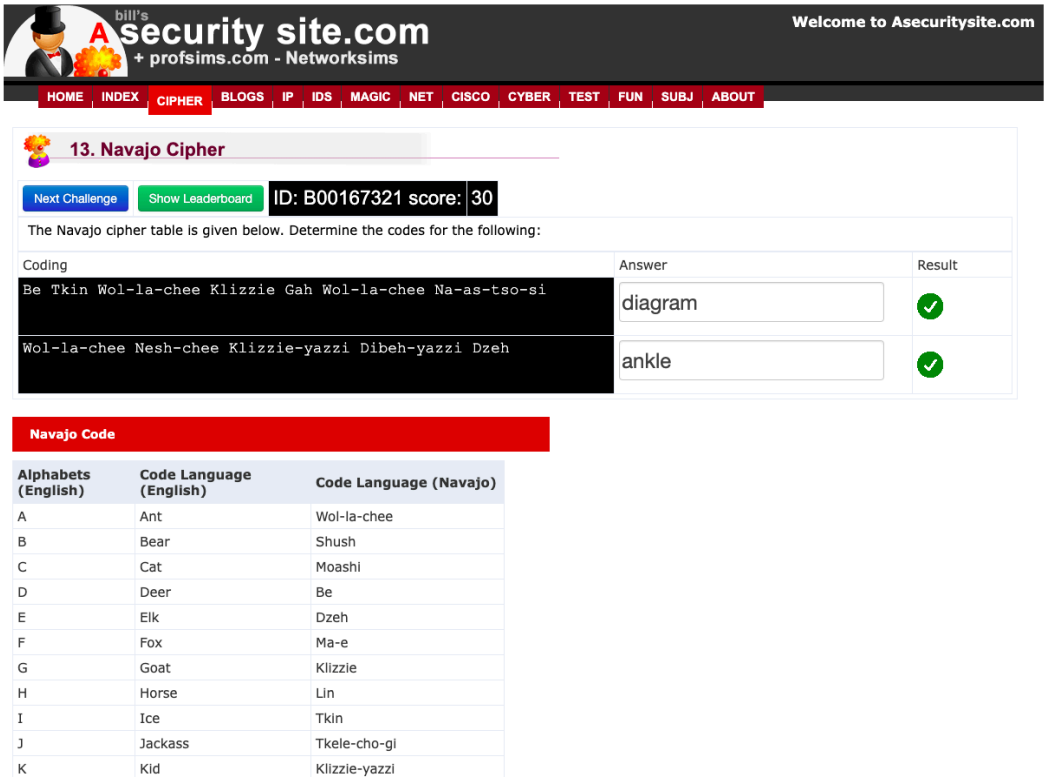
Week 3

Ciphers and Fundamentals (Part 1)

---

30 points score

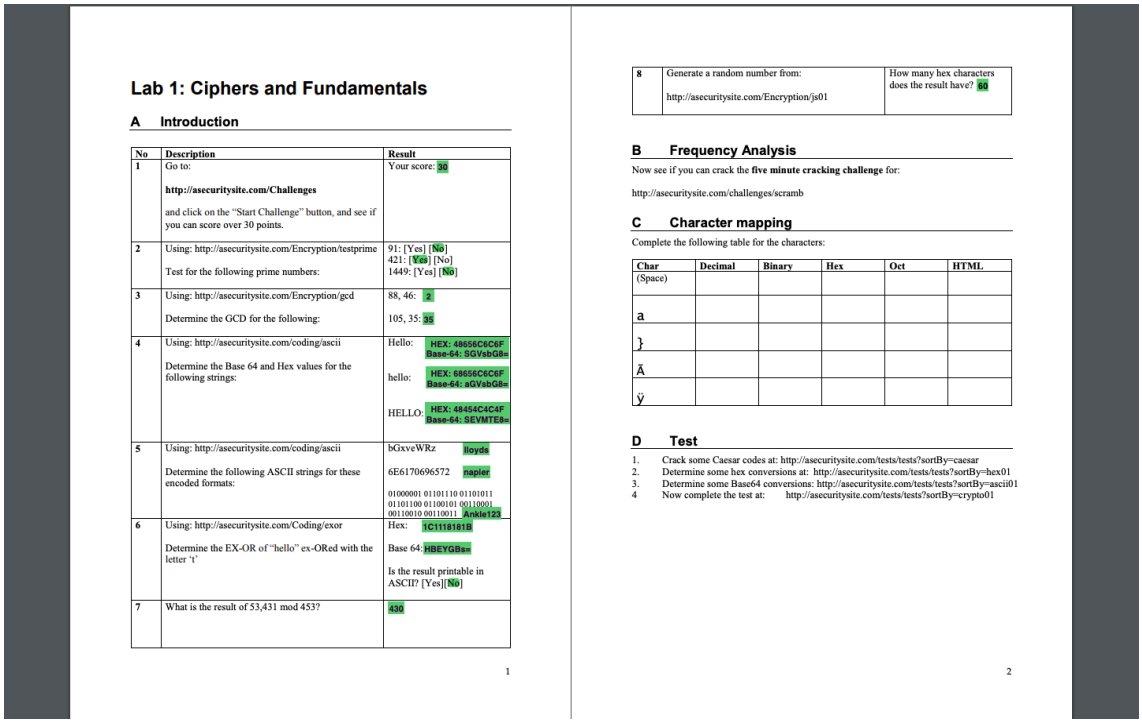
http://asecuritysite.com/Challenges



Alphabets (English)	Code Language (English)	Code Language (Navajo)
A	Ant	Wol-la-chee
B	Bear	Shush
C	Cat	Moashi
D	Deer	Be
E	Elk	Dzeh
F	Fox	Ma-e
G	Goat	Klizzie
H	Horse	Lin
I	Ice	Tkin
J	Jackass	Tkele-cho-gi
K	Kid	Klizzie-yazzi

Sections

A. Introduction



Lab 1: Ciphers and Fundamentals

A Introduction

No	Description	Result
1	Go to: **http://asecuritysite.com/Challenges** and click on the "Start Challenge" button, and see if you can score over 30 points.	Your score: 30
2	Using: http://asecuritysite.com/Encryption/testprime Test for the following prime numbers:	91: [Yes] [No] 421: [Yes] [No] 1449: [Yes] [No]
3	Using: http://asecuritysite.com/Encryption/gcd Determine the GCD for the following:	88, 46: 2 105, 35: 35
4	Using: http://asecuritysite.com/coding/ascii Determine the Base 64 and Hex values for the following strings:	Hello: HEX: 48656C6C6F Base-64: SGVsbG8= hello: HEX: 68656C6C6F Base-64: aGVsbG8= HELLO: HEX: 48454C4C4F Base-64: SEVMTE8=
5	Using: http://asecuritysite.com/coding/ascii Determine the following ASCII strings for these encoded formats:	bGxveWRz lloyds 6E6170696572 napier 01000001 01101110 01101011 01101100 01100101 00110001 00110010 00110011 Ankle123
6	Using: http://asecuritysite.com/Coding/exor Determine the EX-OR of "hello" ex-ORed with the letter 't'	Hex: 1C1118181B Base 64: HBEYGBs= Is the result printable in ASCII? [Yes][No]
7	What is the result of 53,431 mod 453?	430

8	Generate a random number from: http://asecuritysite.com/Encryption/js01	How many hex characters does the result have? 60

B Frequency Analysis

Now see if you can crack the **five minute cracking challenge** for:

http://asecuritysite.com/challenges/scramb

C Character mapping

Complete the following table for the characters:

Char	Decimal	Binary	Hex	Oct	HTML
(Space)					
a					
}					
Ã					
ÿ					

D Test

1. Crack some Caesar codes at: http://asecuritysite.com/tests/tests?sortBy=caesar
2. Determine some hex conversions at: http://asecuritysite.com/tests/tests?sortBy=hex01
3. Determine some Base64 conversions: http://asecuritysite.com/tests/tests?sortBy=ascii01
4. Now complete the test at: http://asecuritysite.com/tests/tests?sortBy=crypto01

B. Frequency Analysis

From this we predict:

- From this I predict that C of your cipher text maps to e in plaintext.
- From this I predict that W of your cipher text maps to t in plaintext.
- From this I predict that I of your cipher text maps to a or o in plaintext.
- From this I predict that Y of your cipher text maps to o or a in plaintext.

1, 2 and 3 letter analysis

One letter (Most pop: a, I)	**Two letter** (Most pop: of, to, in, it, is, be, as, at, so, we, he, by, or, on, do, if, me, my, up, an, go, no, us, am)	**Three letter** (Most Pop: the, and, for, are, but, not, you, all, any, can, had, her, was, one, our, out, day, get, has, him, his, how, man, new, now, old, see, two, way, who, boy, did, its, let, put, say, she, too, use)
a [90]	in [20] of [8] an [20] it [9] is [9] to [3] be [7] or [12] by [4] as [8] if [2] we [3] on [15]	few [1] the [13] has [2] age [3] one [2] new [1] any [5] all [5] our [3] are [1] and [8] for [6] now [2] not [1] use [3]

Enter your guess

This table shows the occurances of the letters in the text (ignoring the case of the letters):

A	B	C	D	E	F	G	H	I	J	K	L	M
x	m	e	d	p	z	h	g	t	k	q	w	s
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
v	i	o	l	f	b	u	y	r	a	j	n	c

Used	To Use
abcdefghijklmnopqrstuvwxyz	--------------------------

Try

Decoded:

in a matter of a few decades the world has changed from an industrial age into an information age. it is one which, unlike earlier ages, encapsulates virtually the whole world. it is also one which allows the new industries to be based in any location without requiring any natural resources, or to be in any actual physical locations. typically all that is required is a reliable network connection. our world is changing by the day, as traditional forms of business are being replaced, in many cases, by more reliable and faster ways of operating. our postal system, while still used for many useful applications, has been largely replaced by electronic mail. with voting, the slow and cumbersome task of marking voting pa-pers with the preferred candidate, is now being replaced by electronic voting. the traditional systems, though, have been around for hundreds if not thousands of years, and typically use well tried-and-tested mechanisms. for the most part, for example, we trust a paper-based voting system, even though it is well known that a count of the votes within an election will often produce different results each time that the vote is counted, and then recounted. an electronic method will, on the other hand, most likely have a success rate of 100%.