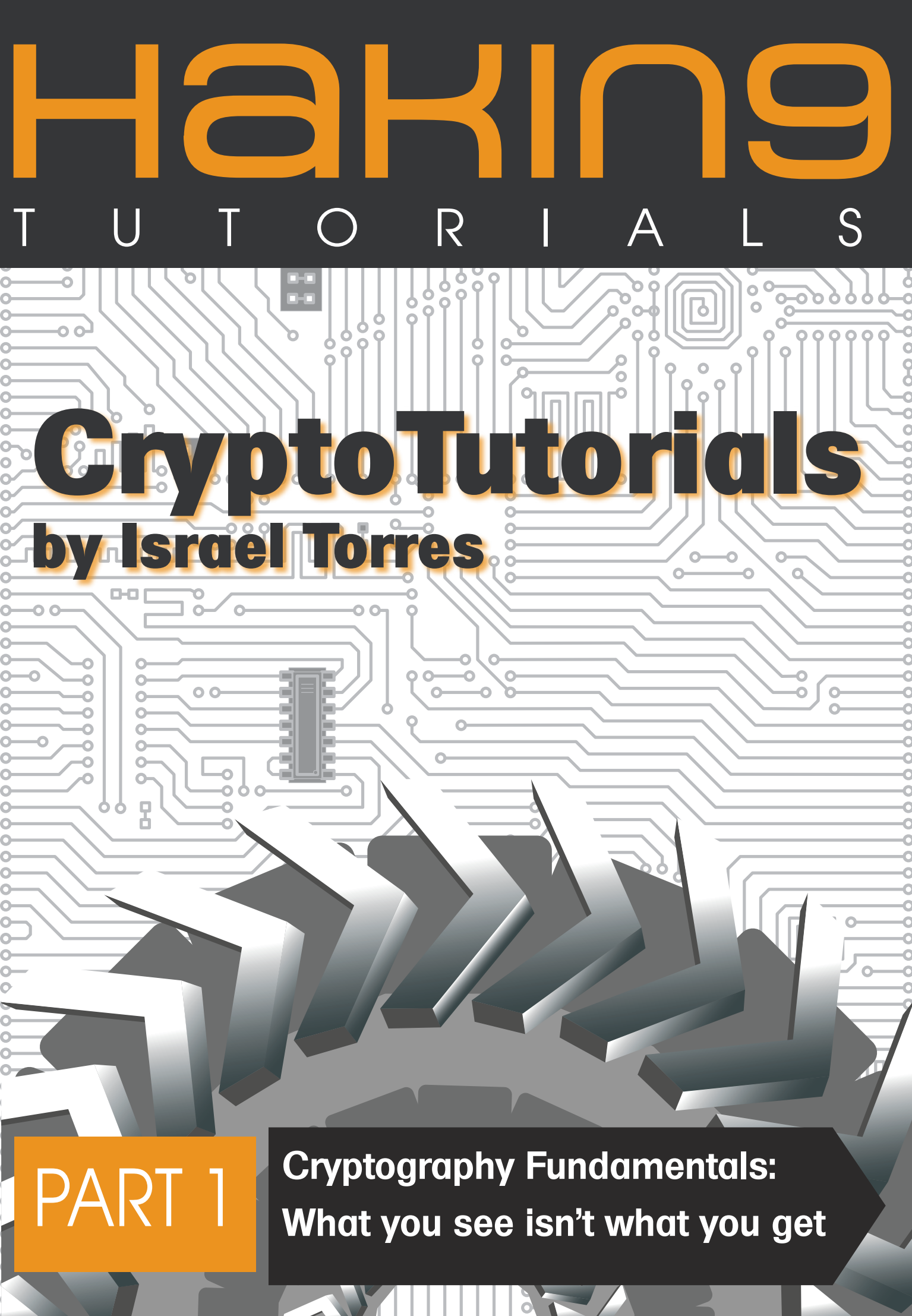
Hacking

TUTORIALS

CryptoTutorials

by Israel Torres



PART 1

Cryptography Fundamentals: What you see isn't what you get

CryptoTutorials

By: Israel Torres

What you will learn...
crypto fundamentals, abstraction, how to keep a secret

What you should know...
basic programming for programmatic implementation

Cryptology is niche study that most of the world feels most comfortable just using without understanding. From the beginning of time people have found the need to keep secrets; very few have succeeded.

In this first tutorial we'll go over many of the fundamental terms as they are defined by various sources. Crypto basically means hidden and ology basically means the study of; put them together (cryptology) and it means the study of things that are hidden. Replace ology with graphy (cryptography) and now you mean things that are hidden in some form of writing. Replace graphy with analysis (cryptanalysis) and now you mean things that are analyzed to be revealed. Another study in a similar realm of hidden messages is steganography (steganos basically means covered) and more so deals with medium concealment (as in what is used for concealment).

A simple example of the difference of cryptography and steganography is as follows :

Crypto may look like this if the word HELLO is shifted by one character to the right of the alphabet [ala simple substitution] (Figure.1): *IFMMP*

Using the bash terminal :

```
echo 'HELLO' | tr 'A-Z' 'B-ZA-A'
```

Stego may look like this if the word HELLO is hidden in plain sight: *His intEntions Lay harmLess Otherwise*. (If you don't see it take ever letter that is uppercase in the order presented and ignore the rest) – naturally using uppercase is obvious but using a slightly different font may be just enough to throw off the analyst.

Using the bash terminal:

```
echo 'His intEntions Lay harmLess Otherwise' | tr -d 'a-z '
```

Lastly it isn't uncommon for both crypto and stego to be used in conjunction to further hide the message from attack/analysis. In this example we hide HELLO using both by first using our shift example from above: IFMMP and then using our uppercase function so the message now appears as: *IF Mother only Moved her Precious artifacts then all would be well*.

Using the bash terminal to decode/decipher/decrypt/extract the original message:

```
echo 'IF Mother only Moved her Precious artifacts then
all would be well' \
| tr -d 'a-z ' | tr 'A-Z' 'Z-ZA-Y'
```

There are even more derivatives involving *code words* that could give the message different meaning based on contextual hints both to help the intended recipient/agent and to thwart the unknown attacker/analyst by confusing keywords like *Mother* to mean the target/mark and *Precious artifacts* to mean the treasure/goal and *all would be well* meaning this action is sanctioned/greenlit and should be proceeded with.

Even with the idea of *code words* there is an extended medium that furthers this from words to images to ideas. There are also traps forged to buy more time – sometimes days and sometimes centuries.

Through the ages such cleverness has won wars and made many victorious and crumbled many empires. Also this has made some very rich and others very poor. Historically this form of science and art has itself been hidden and only really mentioned here and there. Such that most folks (even educated at that) are unaware of its existence and its importance. Within this realm there are the cryptographers and the cryptanalysts that constantly are at war with one another always trying to outwit each other. Within this

	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	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	
					F			I				M			P											

Figure 1. *Simple 1 shift substitution*

Notes

All source code created and tested on:
Mac OS X 10.6.7 10J869
Darwin Kernel Version 10.7.0
GNU bash, version 3.2.48(1)-release

mechanism there is no concept of good versus bad as such is a double-edged sword and both can exist at the same time on the same plane. It really only matters on who uses it and what for. Yes, crypto can be forged to kill and/or save lives. In the world of intelligence such ideas are quite clouded (and really out of the scope of this tutorial). [however we'll play with such notions later in this series]

For the purpose of this tutorial we'll combine the ideas of crypto and stego just as an inclusive of crypto and will really only mention stego when it is dominant in such examples.

Whatever the medium the crypto is applied we all admit it is the year 2011 and in such it is the age of the machine where computers are used to both create and solve cryptographic communications – not sure why the word hasn't evolved further as machines are more of a way to convey our ideas other than in writ. Cryptotypography? Cryptomachina? Hrm, anyway we'll proceed with *cryptography* as not to confuse anyone.

So machines are used to speed up the processes to complicate matters especially in crypto creation so that no naked human can stare at something and get something meaningful from it (if you didn't get that watch the movie Mercury Rising (1998)). With earlier cryptos it was more of a task of memorization and obfuscation than it was computational and algorithmic force. Interestingly it seems that we (as humans) are relying more on computers to do things for us so much so we forget the fundamental of how such things were created in the first place and for why. One would think that no messages could go unencrypted nowadays. We'll leave that argument for the conspiracists. ;)

Such as above; cryptography has many tangents/branches that are rooted deeply into not only history but the future history (futory?) as many secrets that have not been deciphered are just ticking time bombs for the generations ahead that reads uncovers what has not been destroyed/vaporized. It isn't a matter of if something will be decrypted it is only a matter of when.

This concludes this first cryptotutorial and only begins our adventure into cryptology. The subsequent tutorials will expand further as we will cover both breadth and depth in the study of crypto.

Web Links and References

- *http://en.wikipedia.org/wiki/Cryptography*
- *http://en.wikipedia.org/wiki/Stegonagraphy*
- *http://elonka.com/UnsolvedCodes.html*
- *http://en.wikipedia.org/wiki/Category:Uncracked_codes_and_ciphers*

ISRAEL TORRES

Israel Torres is a hacker at large with interests in the hacking realm.

hakin9@israeltorres.org http://twitter.com/israel_torres

Got More Time Than Money?

Try this month's crypto challenge: http://hakin9.israeltorres.org