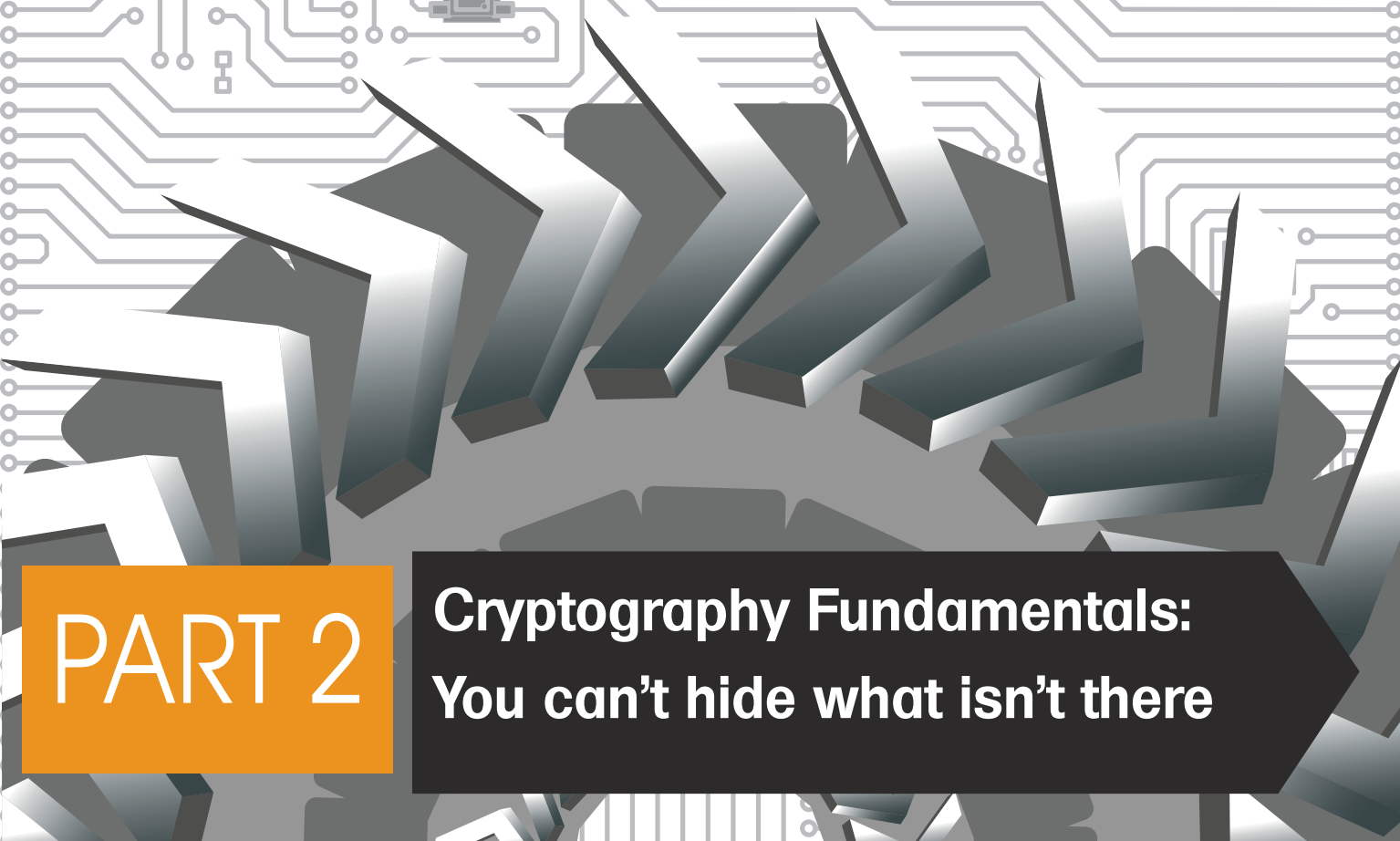
Hacking

TUTORIALS

CryptoTutorials

by Israel Torres



PART 2

Cryptography Fundamentals:
You can't hide what isn't there

CryptoTutorials

By: Israel Torres

What you will learn...

how to make important information nearly invisible to the naked eye

What you should know...

basic obfuscation techniques

The best crypto is the crypto that isn't there. Since it isn't there (wherever there may be) it isn't understood to contain valuable (timely) information and since it isn't understood it isn't attacked (solved). This means that crypto that looks like crypto is a prime target for attack. Crypto that doesn't look like crypto goes by unnoticed; you can't hide what isn't there – at this level there is no need.

As previously discussed in part 1 of this series communication can exist between one or more entities without ever making their existence known even when such entities have intelligence that their communications are being monitored. This is seen at any two points where messages must fall into 'public space' during transit from sender to recipient. One of the best example is the coded communication that occurs in prison systems. Where mixed in various methods are orders to get things done; contraband gotten; kill people.

The evolution of prison communication is quite fantastic as the inmates don't openly have access to computational devices that can assist in making it more difficult for the warden to know what they are up to. Instead the inmates understand their communications (and methodology) are prey to being detected at any time even during a raid while they are creating the message or reading the message. They must then heavily rely on techniques of memorization and obfuscation; not only to hide their messages from the warden but also rival groups within their community if by chance the message is intercepted during transit.

Algorithms and approaches cannot be written down else risk chances of being discovered so only whispers and repetition in person are the best way to generate and store the methodology to encode and decode their codifications. Quite easy as they literally have plenty of time to become studious in this art of memorizing such crafty spells. Those that rely on storing their methods in a non-volatile form are often caught and used as examples to other prison systems to approach things that appear similar (remote communities) thus breaking and discovering larger chains of information (even if it is historical – which may reveal further acts taken place after the fact).

1	ONE	3	1			31	O1	Only I
2	TWO	3	2			32	T2	Troubling Times
3	THREE	5		1		51	T1	Thinking It
4	FOUR	4			1	41	F1	Found It
5	FIVE	4			2	42	F2	Found Twice
6	SIX	3	3			33	S3	Said Third
7	SEVEN	5		2		52	S2	So Twenty
8	EIGHT	5		3		53	E3	Enough Then
9	NINE	4			3	43	N3	Never There
0	ZERO	4			4	44	Z4/O4	Only Four

Figure 1. *Example Obfuscation*

5	Found Twice
3	Thinking It
2	Troubling Times
3	Thinking It
-	
2	Troubling Times
0	Only Four
3	Thinking It
-	
2	Troubling Times
-	
3	Thinking It
-	
2	Troubling Times

Figure 2. *Example Codification*

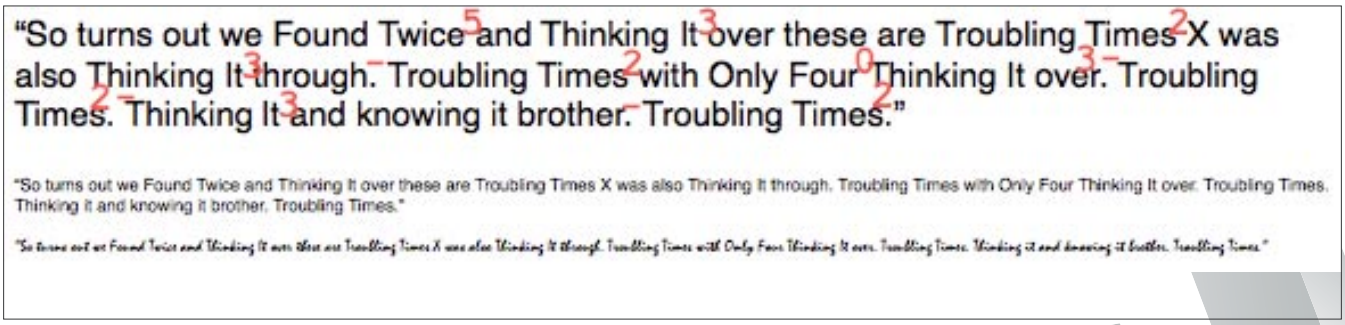


Figure 3. *The Message*

Simple approaches are marking books that are in a 'general library' (or even if bestowed a personal library) whereupon one inmate creates a message or uses a common book as the message generator. Creating the message could be as simple as underlining letters, or poking holes under the significant letters using a small needle-like device easily hidden within the skin. Generating messages by using offsets and indices as legends like a treasure map. For example last digits of ISBN 5323 page 203 paragraph 2 word 3 letter 2 could be hidden in a crib as 5323-203-2-3-2 (the common library may only contain one or two copies of this book making it simpler to keep track of versioning and skewing the information – for example version 2 of a publication could change the meaning entirely – further causing the inmate to insist on a particular version of a book/periodical).

Taking it further to armor the information a secondary process to obfuscate the numbering system (e.g. 5323-203-2-3-2) using an easy to memorize algorithm (Figure 1)

Where

A. Numbers 1 through 0 are spelled out then counted on each letter (ONE contains three letters)

For each repetition of the same count the next same is revised by one (the next three letter word is TWO so it is the second revision of 3 is two (32).

The letter of the first word of the spelled letter remains and the rest is replaced by the revision number (ONE = Letter O Number 1 [O1])

The Letter+Number combination are turned into a partial phrase common in the dialog of the inmates that won't stand out to scrutiny (Figure 2).

Writing this completed message as small as possible (Figure 3) on some type of paper that easily falls apart when digested or flushed making it very difficult for recovery.

It certainly seems time consuming to the average person that multi-tasks throughout a normal work day; however as stated earlier inmates have nothing but time to construe such lengthy schemes especially when they are benefitting from it (cough*bitcoin*cough). Once the message has been comprised and made ready it can then be funneled through means of bartering and simple devices that take advantage of the makeup of the prison design (some of these are really interesting but not part of this focus).

When an algorithm such as the one reviewed above is then set in stone and agreed upon by the parties involved (both internal to the prison and external in the public world) it becomes easier over time in using it quickly and without any type of crib. Imagine it as though looking into the matrix and seeing the lady in the red dress. The problem arises when parties outside the intended party can also see her.

Just because you don't see it doesn't mean it isn't there... On the other side of the bars is the warden's cryptanalyst – trained to detect and decrypt/decode/decipher messages found in transit or in domicile. Some trained better than others and some just really good at it may be able to discern and recognize specific styles to even be able to associate intercepts with specific communities and even people (such as the creator) such as by fingerprinting the algorithm (We'll go over this type of analysis later on down the line in this series) and the psychology involved with it.

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