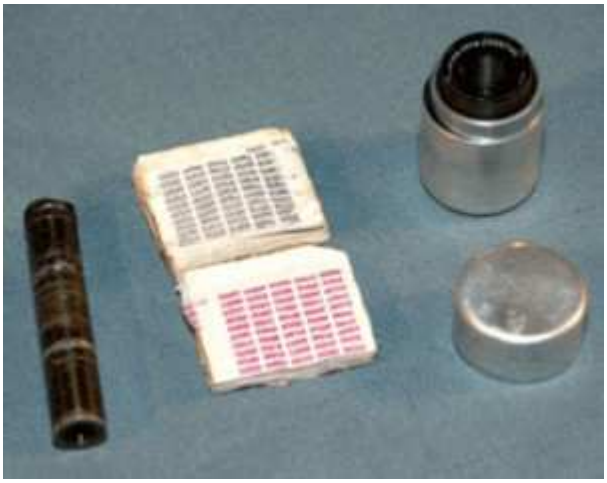
DIY Pencil-and-Paper Encryption

Today we're surrounded by massive computational power and vast communication systems. When you visit your bank's site, you don't think about negotiating cryptographic keys and verifying digital signatures. When you talk on a cell phone, you don't have to worry about COMSEC.

Not too long ago, however, a "computer" was a young woman at a desk, and cryptographic links were short messages. In this article, I'll show you proven, uncrackable encryption scheme that can be done with pencil and paper. If properly implemented, One Time Pad encryption can be used in virtually any medium, and is still used by our favorite black helicopter organizations to conduct missions abroad.

History



What we now call one-time pad encryption (OTP) was patented by Gilbert Vernam at AT&T in 1919 and enhanced by Captain Joseph Mauborgne of the Army's Signal Corps. The earliest military application was reported by the German *Kurzwellenpanorama* magazine in World War

I. Later it was employed by the BBC to send coded messages to Special Operations Executive agents abroad.

The largest application of OTP has been on number stations; these unlicensed, mysterious shortwave radio stations began broadcasting during the Cold War and continue to this day. With a common, inexpensive hardware, an agent anywhere in the world can pickup a broadcast from their organization in an untraceable, uncrackable way. These stations often play musical introductions followed with either Morse code or voice recordings reading alphanumeric code. The Cornet Project has done an amazing job putting together 30 years of recordings of these stations and an informational booklet for free download. If you like spy games, be sure to check it out.

Example

I'll use the example of a Soviet spy. In Moscow, you are issued a tiny booklet of labeled random numbers sequences; this cryptographic key book is identical to one that number station operators have. You sew it into your suit and smuggle it into West Germany. While there, you purchase a shortwave radio and, in the privacy of your flat, listen to the predetermined time and frequency. After a series of beeps, you hear the jingle of music that verifies you are listening to the correct station.

A Russian voice comes on and gives you eight numbers (shown in the table below). Using the first two to identify which code to use, you combine your encrypted message with your key to decode the name of your contact, "Egorov". You rip out the key booklet page and throw it in your fireplace.

Here is the example from above in math form. The encrypted text is what came over the radio, the key is what was in your book.

Encrypted Text	01	03	09	07	*24**	11
Key	04	04	06	11	*17**	11
Decrypted Text	=5=**E**	=7=**G**	=15=**O**	=18=**R**	=15=**O**	=22=**V**

You take your encrypted text (*01-03-09-07-24-11*) and add the key from your book (*04-04-06-11-17-11*). Notice that position five the cipher text and the key sum to 17, not 41. Because there are only 26 letters, it "rotates" around to become 15 (24+17=41. 41-26=17). The encryption process at the number station simply took the message (EGOROV) and subtracted their random key from it, using the same rotating method for negative numbers.

If the key is scientifically random, in theory, the code is impossible to crack. This is because there is no correlation between how the first E is encrypted and the fifth, and a three letter code could just as easily be "CAT" or "DOG". An OTP key is used **only** once, and has a key as long as

the message; if a key is reused, it is possible to mount a computational attack and crack it. Done properly, no previous messages are compromised if a single key is broken (unlike AES or PGP). Furthermore, by keeping the entire process on paper, you minimize the number of mechanism that need to be secure, and thereby reduce the attack vectors. With five minutes of training, you can apply this same system to your IM conversations, email, shortwave radio stations or SMS. Lastly, humans intuitively understand how to hide and secure things, but only conceptually understand firewalls and SSL.

A limitation of OTP is that there's a finite number of messages that can be sent before a new set of keys need to be exchanged. Furthermore, the key exchange has to happen out-of-band and typically in person; this makes the system more inconvenient compared to PGP or AES for computer network communications. Understanding these limitations and advantages, you can build out your own cryptographic implementation easily.

Building Your Own System

Step 1 – Decide on an Alphabet

First we need to figure out how to interpret decrypted messages as English. Often messages are converted into using numbers for their ease-of-calculation in OTP. Numbers don't have to represent just letters, as in the previous example, but also numbers, symbols, words, and syntax. While this the alphabet is not sensitive, per se, it's usually kept with your keys. Here is an example alphabet I've created for text messages.

Code	Meaning	Code	Meaning
01	A	*27*	0
02	B	*28*	1
03	C	*29*	2
04	D	*30*	3
05	E	*31*	4
06	F	*32*	5
07	G	*33*	6
08	H	*34*	7
09	I	*35*	8
10	J	*36*	9

11	K	*37*	(space)
12	L	*38*	.
13	M	*39*	!
14	N	*40*	?
15	O	*41*	AND
16	P	*42*	THE
17	Q	*43*	WHO
18	R	*44*	WHAT
19	S	*45*	WHERE
20	T	*46*	WHEN
21	U	*47*	YES
22	V	*48*	NO
23	W	*49*	MAYBE
24	X	*50*	ABORT
25	Y	*51*	HELP
26	Z	*52*	(End of Message)

Step 2 – Generate Your Key Book

Now we need to generate your key book to smuggle into West Germany. Unlike Hoover's CIA, generating 10,000 new scientifically random numbers doesn't take a room full of agents rolling dice for a week. RANDOM.org is a free service run by the computer science department at Trinity College in Dublin, Ireland; their random numbers are generated from atmospheric noise, and is as close an approximation to random numbers as you can get without a chunk of uranium and a Geiger counter.

Use their SSL-encrypted integer generator to collect your encryption keys. The safest ways to collect these are using Firefox Private Browsing Mode, Google Incognito's window, or encrypt

your hard-drive. If you use spreadsheet software like Excel, be sure to disable autosaving if your hard-drive is unencrypted. Print this and give it to your comrade, preferably on a printer without secret serial number dots.
When you're done, your key book will have pages of labeled two-digit numbers.

Key #	Position 1	Position 2	Position 3	Position 4	Position 5	Position 6	Position 7	Position 8	Position 9	Position 10	Position 11	Position 12	Position 13	
1	87	7	38	43	20	11	84	74	53	35	83	0	80	...
2	20	15	65	20	79	29	15	75	70	87	9	39	55	...
3	17	37	25	64	19	99	33	93	93	49	88	54	69	...
4	77	64	5	96	78	70	68	5	52	78	53	25	98	...
5	56	52	97	30	82	69	31	61	58	49	58	56	80	...
6	57	48	84	48	7	71	87	38	1	27	11	53	51	...
7	20	53	38	91	99	67	43	11	13	1	73	17	47	...
8	10	2	32	52	48	84	51	56	33	29	74	16	44	...
9	87	97	93	58	96	35	31	89	50	57	73	32	52	...
10	57	99	1	33	52	2	40	77	9	31	67	39	62	...

Step 3 – Transmit

When you transmit, you have lots of options available to you today your granddaddy didn't. Your globally-connected encrypted pocket radio (cell phone) and SMS are fantastic systems, albeit expose your geographic location to the service provider. If you want to transmit a message to many people/agents, a Twitter or Blogger account posted to via Tor or a pre-paid cellphone create the modern day equivalent of a number station. In fact, there is at least one known bot net coordinated via an anonymous Twitter account (not encrypted, however).

That's it, no more tools or training is required. While OTP certainly has its limitations, under the right circumstance it can outperform more sophisticated (and more difficult) cryptographic systems. Anyone with five minutes of training and a piece of paper can use the same tools the CIA, KGB, and Mossad use to conduct operations abroad. It's up to you to learn how to apply these in your own situation, but remember that many times, the simplest tool in your arsenal is the most powerful.