Introduction to Network Security – Part 6

Posted by Alejandro G. Carlstein Ramos Mejia on November 2, 2010 November 4, 2010 About Programming / Network Security

NOTIFICATION: These examples are provided for educational purposes. The use of this code and/or information is under your own responsibility and risk. The information and/or code is given 'as is'. I do not take responsibilities of how they are used.

Poly-alphabetic Cipher

In the previous posting, we say that the mono-alphabetic cipher instead of shifting the alphabet a number of letters (Caesar cipher), its substitute each letter arbitrarily by mapping the plaintext letter map to a random arranged ciphertext. The only requirement for the ciphertext was that the letters must not be repeated. Now we are going to see a cipher that uses a set of related mono-alphabetic rules plus a key to determine which rule will be use to perform a transformation.

Vigenère Cipher

Encryption:

This cipher is similar to the Caesar cipher for the use of the 26 letters alphabet with the only different that we create a table in which:

1. The columns represent the plain text
2. The rows represent the key
3. The alphabet inside the table is shifted to the right one letter one time for each letter of the alphabet key.

To be more clear, let take a quick look of the Caesar cipher table:

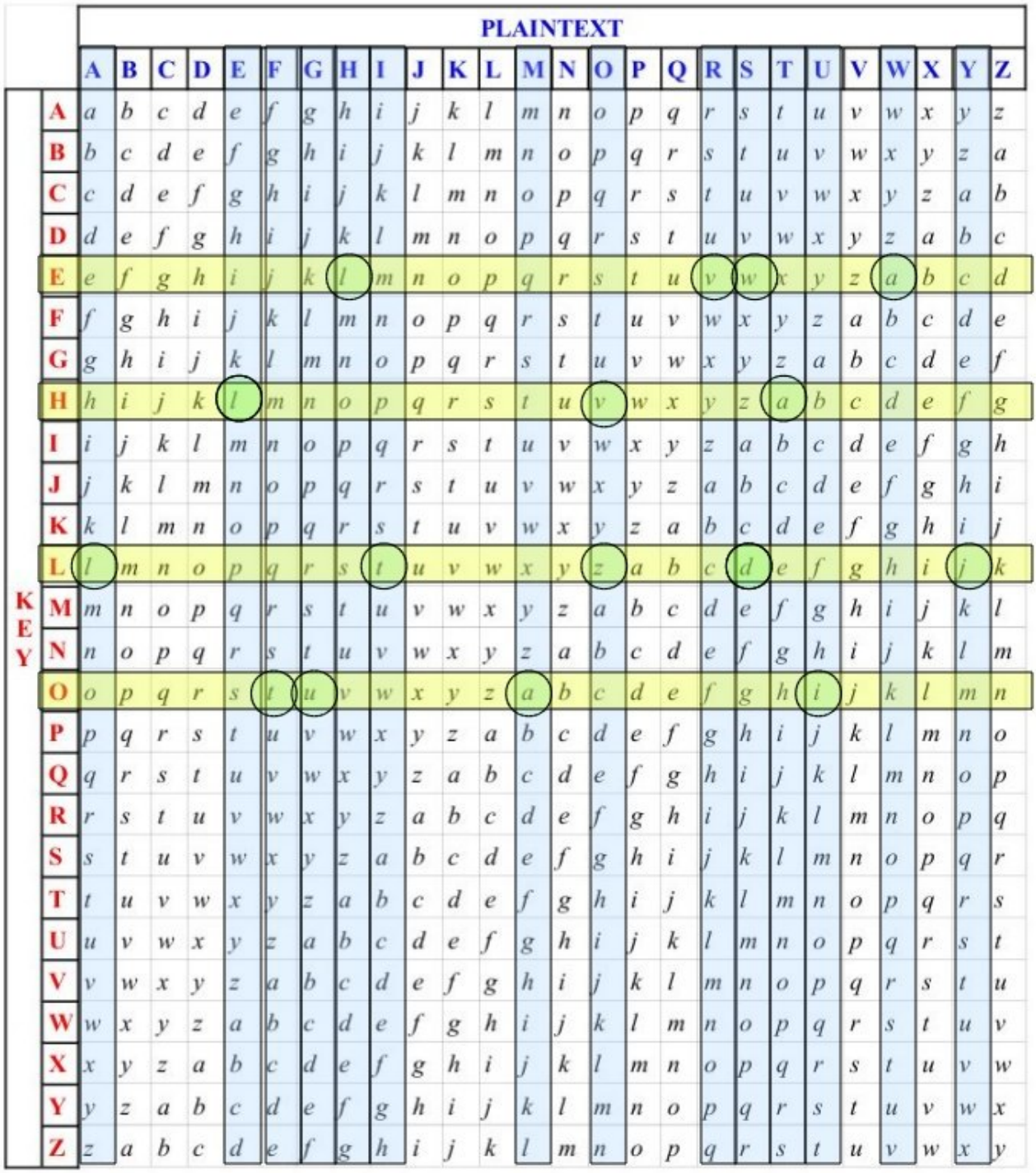
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

In this example, We started the alphabet on the letter 'E' because the key was 5.

Now, the Vigenère Cipher will apply this shifting 26 times, one time per row, for each letter of the alphabet that correspond to the key as follow:

		PLAINTEXT																								
		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
KEY	A	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
	B	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
	C	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
	D	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
	E	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
	F	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
	G	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
	H	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
	I	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
	J	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
	K	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
	L	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
	M	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
	N	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
	O	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
	P	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
	Q	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
	R	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
	S	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
	T	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
	U	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
	V	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
	W	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
	X	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
	Y	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
	Z	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

Lets say that you have the following key “THIS MESSAGE WAS FOR YOU”, and your key is “HELLO” then using the table:



PLAINTEXT	T	H	I	S	M	E	S	S	A	G	E	W	A	S	F	O	R	Y	O	U
KEY	H	E	L	L	O	H	E	L	L	O	H	E	L	L	O	H	E	L	L	O
CIPHERTEXT	a	l	t	d	a	l	w	d	l	u	l	a	l	d	t	v	v	j	z	i

We would obtain:

From a mathematical point of view we have:

1. Lets assume that we take the letters of the alphabet from A to Z and be replace

them with number starting from 0, for example: A = 0, B = 1, ..., Z = 25.
2. Since we have 26 letters in the alphabet, lets perform module of 26 on this equation.
3. If 'i' is the letter position, P indicate the plaintext, K indicate the key, and C indicate the ciphertext then:

$$C_i \equiv (P_i + K_i) \pmod{26}$$

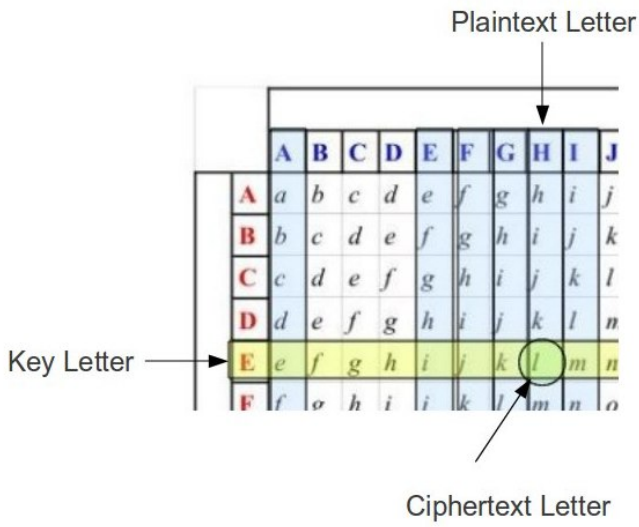
(For more information about the algebra involved in the Vigenère cipher: http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher)

Decryption

For decryption we only need to use a letter of the key to identify the row and the letter of the ciphertext in the row to identify the column, the letter designated to the column give us the plaintext letter.

From a mathematical point of view we have:

1. Lets assume that we take the letters of the alphabet from A to Z and be replace them with number starting from 0, for example: A = 0, B = 1, ..., Z = 25.
2. Since we have 26 letters in the alphabet, lets perform module of 26 on this equation.
3. If 'i' is the letter position, P indicate the plaintext, K indicate the key, and C indicate the ciphertext then:



$$P_i \equiv (C_i - K_i) \pmod{26}$$

(For more information about the algebra involved in the Vigenère cipher: http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher)

Security

This cipher is not secure. If two or more sequences are identical inside the plaintext, we run the risk that identical ciphertext sequence will be generated. The attacker can use these repetition in the ciphertext to make a deduction about what is the plaintext. The more plaintext is needed to encrypt, the more chances that the ciphertext can be broken or the key found.

As an example, lets assume we have the following:
Plaintext: WE RUN WHEN WE WERE DISCOVER BY THEM
Key: RUNNING NO RUNNING NO RUNNING NO

This would give us a ciphertext in which we can spot the repetitions:

W	E	R	U	N	W	H	E	N	W	E	R	E	D	I	S	C	O	V	E	R	B	Y	T	H	E	M	Plaintext
R	U	N	N	I	N	G	N	O	R	U	N	N	I	N	G	N	O	R	U	N	N	I	N	G	N	O	Key
N	Y	E	H	V	J	N	R	B	N	Y	E	R	L	V	Y	P	C	M	Y	E	O	G	G	N	R	A	Cipher text

The only way around this problem is by using the Autokey cipher.

Autokey Cipher

An auto-key cipher is the concept of generating a key that does not have a repetition cycle.

Instead of having a plaintext and a key such as this example:
Plaintext: WE RUN WHEN WE WERE DISCOVER BY THEM
Key: RUNNING NO RUNNING NO RUNNING NO

We could have the following key:
Plaintext: WE RUN WHEN WE WERE DISCOVER BY THEM
Key: RUNNING IS NOT THE SOLUTION THIS

This would give us a ciphertext with no repetitions:

W	E	R	U	N	W	H	E	N	W	E	R	E	D	I	S	C	O	V	E	R	B	Y	T	H	E	M	Plaintext
R	U	N	N	I	N	G	I	S	N	O	T	T	H	E	S	O	L	U	T	I	O	N	T	H	I	S	Key
N	Y	E	H	V	J	N	M	F	J	S	K	X	K	M	K	Q	Z	P	X	Z	P	L	M	O	M	E	Cipher text

One-Time Pad Cipher

The One-Time Pad cipher use a similar concept as the Auto-Key Cipher; however, the difference is the generation of a random key which is as long as the message. Also, it is required that at the end of the transmission, the random key generated must be destroyed.

The only problem is to find a secure way to distribute the random generated key between the principals.