MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

One-Time Pad with flaws

Author: Bernhard Esslinger

November 2010 (Update January 2012)

One-Time Pad

The “Three Investigators” heard that it is possible to create truly unbreakable cipher texts if you link a stream of true random numbers to the plaintext (one-time pad).
The link operation can be created bytewise when using the Vigenère cipher (for example addition of the corresponding numerical values modulo 26) or by using XOR (exclusive OR of the individual bits).

Since then the “Three Investigators” have encrypted their messages to each other using the Vigenère cipher to combine the different characters. Their plaintexts only consist of the 26 capital letters of the alphabet. As random numbers they use a random number sequence.

One-Time Pad

The ciphertext is calculated as follows:

Assignment: Letter – Value

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Example plaintext: T E X T = 19 4 23 19

Example of a random number sequence = key stream:

16, 8, 17, 23, 0, 3, ...

Sample ciphertext: (19+16) mod 26 = 35 mod 26 = 9 = J

(4+8) mod 26 = 12 mod 26 = 12 = M

(23+17) mod 26 = 40 mod 26 = 14 = O

(19+23) mod 26 = 42 mod 26 = 16 = Q

Challenge

This is an easy method that can be accomplished with paper and pencil. However, it is very difficult to generate a truly random key-stream (with or without a computer).

Therefore, the "Three Investigators" considered thinking about a number and using it as starting value for an infinite, random number sequence. It should be easy for the transmitter and the receiver to generate or obtain this number sequence.
Instead of a book they chose the mathematical constant PI = 3,14159265358979323846264338327950288419716939937510582097494459230781640 62...

Challenge

They agreed to use the offset in the key stream as key (e.g. offset 7 is the digit "6"). From then on they took the following key stream and always grouped 2 digits as one number for the random number sequence.
With an offset of 7 the key stream would be: 53, 58, 97, 93, 23, ...

To ensure this method did not become too complicated, the “Three Investigators” agreed to use only short messages. Additionally, they agreed not to make their offset greater than 100, and to often change the key.

Challenge

Now you know the method, but not the key. Do you think you can, nevertheless, decrypt an eavesdropped encrypted message (see file *mtc3-esslinger-06-onetimepad-cipher.txt*)?

The solution consists of the whole plaintext (containing a quote), the last name of the real author of the quote, and the offset used. Please write everything in sequence, and always write in capital letters.