CS: Excersise 1

1005086k George Kouzmov

1 KPT

colum1	column2
0xacee	0xc5bd
0x9af8	0x88f3
0x87e9	0x8dbd
0x80fc	0x88bd
0x85bd	0x9efc
0x8cec	0x9ae9
0x9cf4	0x8cff
0x99f0	0x88ee
0x8cf3	0x82f8
0x9dbd	0x9db3
0x8ff2	0xc9bd
0x9bbd	0xb9f5
0x88bd	0x80f1
0x84fc	0x86ee
0x9df5	0x86ed
0x8cf0	0x81f8
0x88e9	0x9bee
0x80fe	0xc9f9
0x80fc	0x86bd
0x87bd	0x87f2
0x8af2	0x9dbd
0x87ee	0x87f8
0x80ee	0x8cf9
0x9dee	0xc9e9
0xc9f2	0x81f8

0x8fbd	0xc9ea
0x99f8	0x88ee
0x87b1	0x9df8
0xc9ed	0x8bfc
0x88ed	0x9af6
0x8cef	0x8ce9
	0xe39d

For the dataset above with known plain text *0x4573* that is equal to the first enrcypted block *0xacee* after brutefocing through passing for every key in range 0 to 65536 (range of 16 bit int) we find that

Key Integer : 47899

Key Hex :0xbb1b

Text: Essential equipment for a mathematician consists of pen, paper, and a wastebasket. Philosophers do not need the wastebasket

2 CTO

column1	column2
0x887f	0xb478
0xb364	0xa97b
0xb937	0xb879
0xab7f	0xfb63
0xb337	0xfc7e
0xaf76	0xb263
0xa537	0xb965
0x9563	0xae62
0xfb7b	0xac63
0xb037	0xfc63
0xb272	0xb478
0xaa72	0xaf72
0xae37	0xfc73
0xab78	0xb37e
0xae7c	0xb270
0xfc64	0xfc7e

0xa81d

For the dataset above with unknown plain text we extract the data through a dictionary. For each key the text blocks are decoded word by work until a 'space' character is found so a word can be identified and later on it's compared with a dictionary if it's an english word, the probability is incremented and the loop is continued untill a non english word is found. This was the result found:

Key Integer : 32785

Key Hex :0x8011

Text: Those who say It'll never work shouldn't interrupt those doing i

However through the process another close to english language sentence was found that was readable by the human eye and understandable however it had mixed length characters and not existing asii printable characters that looked like this:

Key Integer : 24593

Key Hex :0x6011

Text: thOsE WhO SaY it[invalid char]lL NeVeR WoRk sHoUlDn[invalid char]t iNtErRuPt tHose dOiNg i

However the probability of the sentence is lower then the correct one hence the first one was correct. After some analyisis it was found that after the seventh block of the block text we could find unambiguous english sentence. Even though the other sentence is readable it is not correct english language.

3 TMT

column1	column2
0x887f	0xa97b
0xb364	0xb879

0xb937 0xfb63
0xab7f 0xfc7e
0xb337 0xb263
0xaf76 0xb965
0xa537 0xae62
0x9563 0xac63
0xfb7b 0xfc63
0xb037 0xb478
0xb272 0xaf72
0xaa72 0xfc73
0xae37 0xb37e
0xab78 0xb270
0xae7c 0xfc7e
0xfc64
0xb478

For the dataset with plain text known equal to *0x4120* a table was generated using the chain rule. The parameters I used were N = 45000 and L = 500. The generated table was saved to a file which was later read. In the file a for loop goes through each textblock when a text block is found in the table the chain rule is done for L-1 times to find the key and then the key is used do decrypt the text.

Key Integer : 17671

Key Hex :0x4507

Text: A day can really slip by when you're deliberately avoiding what you're supposed to d