Group D

[redacted]

*Introduction*

We were approached by OCRAI with a request to design a method of encryption that could be applied to ordinary employee communications and other typical text files. This algorithm is meant to be secure and efficient for encrypting and decrypting English messages so that important information is not leaked. Per the request of OCRAI this is a novel non-standard method of encryption developed specifically for their needs.

*Methods*

The method for encryption which we used is based on the principle that any number has a distinct factorization into prime numbers, up to order. When we receive the data, we first assign each of the 26 letters with the corresponding lowest prime number. The prime numbers used for this are not part of the key, but are instead common knowledge. A = 2, B = 3, …, Z = 101. Additionally, each of the 10 numerals were assigned the 27-36th smallest prime numbers. Therefore, 0 = 103, 1 = 107, …, 9 = 151. We then break apart the plaintext into "words", with any non-letter/number serving as a delimiter. As an example, the phrase, "I don't 100% know if I love you yet, but you're pretty neat I guess" will break into the words: "I" "don" "t" "100" "know" "if" "I" "love" "you" "yet" "but" "you" "re" "pretty" "neat" "I" "guess". Note that all delimiters, including spaces and punctuation, will be passed into the ciphertext unaltered.

We then take each word, convert each character of the word into the corresponding prime, and output the product of the characters plus a 5-digit number which serves as our key. As an example, if our key is 12345, then the word "cab" becomes "5 * 2 * 3" = "30" (C = 5, A = 2,

B = 3) and, adding the key, becomes “30 + 12345” = “12375”. The only problem is that the receiver of that word, “30”, can obtain the letters “ABC”, but won’t know the order they need to go in. For that reason, we have added a number in the ciphertext which indicates the proper permutation of the letters. Let the word be organized as a list of addresses, similar to a string. Therefore, in the word “CABBY0”, the letter C is in address 0. The letter A is in address 1. The letter B is in address 2. The letter B is also in address 3. The letter Y is in address 4. The numeral 0 is in address 5. In our ciphertext, we have included a number following each “word” which shows the proper permutation of the characters by showing the addresses of each letter, from the largest corresponding prime number to the smallest corresponding prime number. We also add a 0 at the beginning of the permutation to distinguish it from the “words”.

For example,

We convert “CABBY0” to its primes, “5 * 2 * 3 * 3 * 97 * 103”.

We multiply our primes together, “899190”.

We add our cypher key, “899190 + 12345” = “911535”.

We add our permutation, “0540231”.

We send the message “911535 0540231” to Bob.

Bob breaks the word, 911535, into the primes “2 * 3 * 3 * 5 * 97 * 103”.

Bob then converts those primes into the characters, “A, B, B, C, Y, 0”.

Bob then takes the permutation number (0540231), removes the beginning 0 (540231), and matches the addresses to the characters, “A = 1, B = 3, B = 2, C = 0, Y = 4, 0 = 5”.

Therefore, the order of the letters becomes “C = 0, A = 1, B = 2, B = 3, Y = 4, 0 = 5”.

Bob then has the message, “CABBY0”.

Another example is the sentence, “I 100% know how to decrypt this.”

Which becomes the primes, “23  103 * 103 * 107  31 * 43 * 47 * 83  19 * 47 * 83  47 * 71  5 * 7 * 11 * 53 * 61 * 71 * 97  19 * 23 * 67 * 71”.

Which is sent to Bob as, “12368 00 1147508 0012% 5212378 03210 86464 0210 15682 001 8572295680 04635102 2091154 00321.”

Which becomes, “I 0 010 012% KNOW 3210 HOW 210 OT 01 CDEPRTY 4635102 HIST 0321.”

And is decrypted to finally show, “I 100% know how to decrypt this.”

In summary,

Take the message and convert every character in each word into primes. Multiply those primes together. Add the key, which is as a 5-digit number, to each word. After each number, include the permutation of those letters, which is a list of addresses for each character in the order from largest to smallest. Then send the message. The decrypter subtracts the key from each word, finds the prime factors of each word, and sorts each word into its characters. The decrypter then changes each word into its proper form through the permutation given after each word. This cryptosystem is, of course, not without flaws or weaknesses. The cipher could be strengthened if a slightly longer key was used which would designate a rule as to which prime corresponds to which letter instead of simply using a public listing. As it is, however, we deem that the described method of encryption will be sufficient for all of OCRAI’s data protection needs.

List of Primes:

A 2

B 3

C 5

D 7

E 11

F 13

G 17

H 19

I 23

J 29

K 31

L 37

M 41

N 43

O 47

P 53

Q 59

R 61

S 67

T 71

U 73

V 79

W 83

X 89

Y 97

Z 101

0 103

1 107

2 109

3 113

4 127

5 131

6 137

7 139

8 149

9 151