HOMEWORK 5

Due on 4/30, submit in HARDCOPY

1. (15%) Decipher the following ciphertext, which was encrypted with the Caesar cipher: TEBKFKQEBZLROPBLCERJXKBSBKQP. Follow the example in Chapter 8.2.2 to find the key and the plaintext, and show the table in Figure 8-2 for this question. Make a program to compute the table (but no need to submit your program).

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P
Plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

TEBKFKQEBZLROPBLCERJXKBSBKQP
Wheninthecourseofhumanevents

Inserting spaces in all the appropriate places we have the final plaintext

When in the course of human events

2. (10%) Let k be the encryption key for a Caesar cipher. Then, the decryption key is 26-k. One of the characteristics of a public key system is that the encryption and decryption keys are different. Why is the Caesar cipher not a public key system, even though its encryption and decryption keys are different?

Because in a Caesar cipher if you have the encryption or decryption key you can get the other and by only possessing one key. While in a public key system owning either key does not grant you access to the other, making it the more secure system.

3. (15%) We have a law: (ab)%n = ((a%n)(b%n))%n. We want to compute (35^77)%83, i.e. 35 powers to 77 then modulo over 83.
(a) Show how to use the law to reduce the number of multiplications of this computation from 76 multiplications to 9 multiplications.

35^1
35^2 = 1225mod83 => 63mod83
35^4 = (35^2)^2 = (63^2)mod83 = 3969mod83 => 68mod83
35^8 = (35^4)^2 = (68^2)mod83 = 4624mod83 => 59mod83
35^16 = (35^8)^2 = (59^2)mod83 = 3481mod83 => 78mod83
35^32 = (35^16)^2 = (78^2)mod83 = 6084mod83 => 25mod83
35^64 = (35^32)^2 = (25^2)mod83 = 625mod83 => 44mod83

(b) Make a C or C++ or Java program to implement an integer exponentiation function dexp(unsigned int x, unsigned int y, unsigned int n) that returns (x^y)%n with reduced multiplications. Copy and paste your code in your homework submission.

```
template <typename T>
T modpow(T base, T exp, T modulus) {
  base %= modulus;
  T result = 1;
  while (exp > 0) {
    if (exp & 1) result = (result * base) % modulus;
    base = (base * base) % modulus;
    exp >>= 1;
  }
  return result;
}
```

(c) Use your program to get the result of (35^77)%83. Show the result.

Result is 27.

4. (10%) A byte-sum program exclusive or's all bytes in its input to produce a one-byte hash. Is this byte-sum program a secure hash function or not? Show one example of inputs to justify your answer.

Not a secure hash function, being that the output produced is always 1 byte that is of 8 bits hence it is always going to be easy for the attacker to find 2 inputs producing the same hash in roughly O(24) operations.

For example by assuming that key is all 1's and first 8 bits will be taken from the resulting output as our hash Now say input is 101010101010.Key will be of length of input that is 12 and all 1 bits Therefore 101010101010 xor 111111111111 = 010101010101 Therefore hash(first 8 bits) = 01010101
Now consider the input - 101010101111 Key will be of length of input that is 12 and all 1 bits Therefore 101010101111 xor 111111111111 = 010101010000 Therefore hash(first 8 bits) = 01010101

Note that same hash is produced for 2 different inputs approving that hash function is not secured.

5. (10%) Multiply two large numbers p and q (you will need to find a tool or a library by yourself)

p =
0xc315d99cf91a018dafba850237935b2d981e82b02d994f94db0a1ae40d1fc7ab9799286ac68d620f1102ef515b348807060e6caec5320e3dceb25a0b98356399

q =
0xe90bbb3d4f51311f0b7669abd04e4cc48687ad0e168e7183a9de3ff9fd2d2a3a50303a5109457bd45f0abe1c5750edfaff1ad87c13eed45e1b4bd2366b49d97f

p * q = **b197 d3af e713 8165 82ee 988b 276f 6358 00f7 28f1 18f5 125d e1c7 c1e5 7f27 3835 1de8 ac64 3c11 8a54 80f8 67b6 d875 6021 9118 18e4 7095 2bd0 a526 2ed8 6b4f c4c2 b796 2cd1 97a8 bd8d 8ae3 f821 ad71 2a42 285d b67c 8598 3581 c4c3 9f80 dbb2 1bf7 00db d2ae 9709 f7e3 0776 9b5c 0e62 4b66 1441 c1dd b62e f1fe 7684 bbe6 1d8a 19e7**

6. (10%) Factorize a short large number (you will need to download and use the tool yafu)

N=359567260516027240236814314071842368703501656647819140843316303878351

59 567260 516027 240236 814314 071842 368703 501656 647819 140843 316303 878351 (69 digits) = 17963 604736 595708 916714 953362 445519 (35 digits) × 20016 431322 579245 244930 631426 505729 (35 digits)

Möbius: 1

$n = a^2 + b^2 + c^2 + d^2$

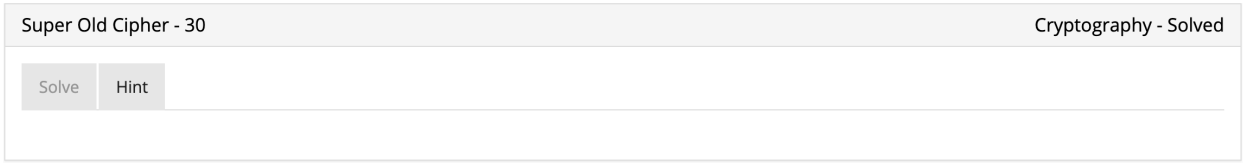
a = 14289 016215 761299 320744 668512 106427 (35 digits)

b = 10797 671605 230392 476974 632177 292689 (35 digits)

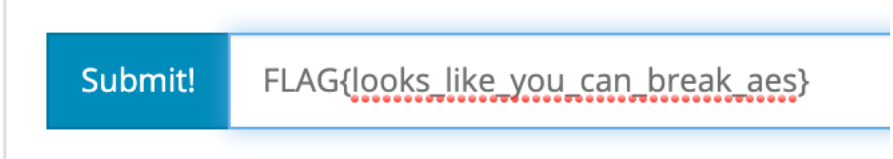
c = 5553 744391 295291 603970 848491 758201 (34 digits)

d = 2820 901849 319697 198195 560861 354070 (34 digits)

7. (10%) Run the CTF virtual box, read the partial solution of "Super Old Cipher". Show the flag.



8. (10%) Run the CTF virtual box, read the partial solution of "Messy AES". Show the flag.



MUYSHONDT, ALEXANDER D
4/30/19

HOMEWORK 5

Messy Aes - 30	Cryptography - Solved

Solve Hint