MATH 8
ASSIGNMENT 15: RSA ENCRYPTION

JAN 28TH, 2018

In one weeks we are going to start Geometry. Please buy: "The Art of Problem Solving, Volume 1: The Basics" by Sandor Lehoczky and Richard Rusczyk, ISBN-13: 978-0-9773045-6-1. Please do not get the solution manual (or hide it for emergencies). It is important that you try the problems on your own.

1. Encryption

In order to encipher messages involving letters, we need to define numerical equivalencies for the alphanumberical letters. Here we will only use upper case letters.

Letter	Numerical Equivalent	Letter	Numerical Equivalent
A	00	N	13
B	01	O	14
C	02	P	15
D	03	Q	16
E	04	R	17
F	05	S	18
G	06	T	19
H	07	U	20
I	08	V	21
J	09	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

Table 1. Table to convert characters to numerical equivalent

1.1. **public encryption key.** Let p and q be distinct odd prime numbers (typically very large), let $m = pq$, and let e be a positive integer such that $gcd(e, \phi(m)) = 1$. The ordered pair (e, m) is the public encrytion key.

1.2. **formatting.** Translate each letter of the plaintext into its two-digit numerical equivalent from the table. Format these numerical equivalents into blocks of maximal even length such that each block of digits, viewed as a single poitive integer, is less than m. If the final block contains fewer than the required even number of digits, then "dummy" digits, say 23's (fot X's) are added so that this block has sufficient digits.

1.3. **The encryption scheme.** Encipher each block P, when viewed as a single positive integer, via

$$P^e \equiv C \mod m, 0 \leq C \leq m \tag{1}$$

to obtain a new block C, which is viewed as a single positive integer.

2. Decryption

2.1. **The Private Decryption Key.** Let (e, m) be the public encryption key. The ordered pair (d, m) is the private decryption key where d is the inverse of $e \mod \phi(m)$

2.2. **The Description Scheme.** Decipher each block C, which is viewed as a single positive integer, via

$$C^d = P \mod m, 0 \leq P \leq m \tag{2}$$

to obtain a new block P of maximal even length, such that each block of digits, when viewed as a single positive integer, is less than m.

2.3. **Deformatting.** Replace each two-digit block with its alphabetical equivalent from Table. Deformat the resulting blocks of letters into a meaningful message, truncating dummy digits.

3. Assignments

3.1. **Encryption.** Create a message of up to 16 characters (not including spaces) to send to the other group. You can use either of these public encryption pairs: $(11, 3127)$, $(11, 2623)$, or $(13, 2419)$

3.2. **Deliver message.** Give the encrypted message together with the encryption pair to the other group.

3.3. **Decrypt message.** First you have to figure out the prime factorization of m for the encryption key, then you need to calculate $\phi(m)$ and then take the inverse of $e \mod \phi(m)$ to get your private decryption key d. Then proceed to the decryption.

4. Proof the RSA Scheme of encryption/decryption

Show that if $C^d \equiv P \mod m$ then $P^e \equiv C \mod m$ given that d is the inverse of $e \mod \phi(m)$.

5. Security of RSA Encryption

Perhaps the most intriguing feature of the RSA encryption system is the fact that knowlegde of the public encryption key (e, m) does not lead to the knowledge of the corresponding decryption key (d, m) in a realistic period of time. Since d is the inverse of $e \mod \phi(m)$, the computation of the decryption key d requires the computation of $\phi(m)$. If the two component prime numbers p and q are known, this computation of $\phi(m)$ is ridiculously easy: $\phi(m) = \phi(p)\phi(q) = (p-1)(q-1)$. However, the component prime numbers of m are only known to the inended recipient of the message. Persons other than the recipient would have to compute $\phi(m)$ given m only, and this computation may be prohibitive. For example, if each component prime number of m has 150 digits, then m has approximately 300 digits. If the computer that we are using can perform 10^9 operations per second than this task would take approximately $5x10^{12}$ years!