Program 5: RSA

CPSC370: Introduction to Computer Cryptology

Due Wdnesday, December 7, 2016 11:59PM

In this programming assignment, you are asked to write C/C++/Java codes to implement encryption/decryption functions for RSA discussed in class.

1 Details of the program

1. Implement the following functions for your RSA:
   (a) Mapping function from alphanumerical characters to decimal digits (See textbook Figure 9.7.(b) and `MappingRSA.pdf` for mapping). Every two alphanumerical characters will be converted to a block used in RSA encryption and decryption.
   (b) Key generation function that takes int the inputs of two prime numbers, `p` and `q`, and generate the parameters $(n, \phi(n), e, d)$, and the keys for RSA. The following sub-routines may be implemented:
   - GCD function to find e: $gcd(\phi(n), e) = 1; 1 < e < \phi(n)$. Since there could be many such e values, you may use *gcd* to find the first five such e values.
   - Multiplicative inverse: $d = e^{-1}(\text{mod } \phi(n))$. You may use extended Euclidean algorithm to find the first five such d values corresponding to each of five e values (**Note**: Your multiplicative inverse value should be within $[0, \phi(n))$).

   (c) Encryption function that takes each block of plaintext and public key.
   (d) Decryption function that takes each block of ciphertext and private key.
   (e) Mapping function from decimal digits back to alphanumerical characters.

2. Experiment the correctness of your program by using the following plain text and prime numbers, $p = 73$ and $q = 151$:
   (a) plain text: `How are you?`
   (b) plain text: `Public key cryptography.`

   For each test of your RSA algorithm, you need to output the following information:
   (a) RSA key information: $n, \phi(n)$, the first five e, and d values
   (b) Original plain text

(c) Five sets of:
    - Public key
    - Ciphertext
    - Private key
    - Plaintext

(d) Decrypted plaintext from decimal digits back to alphanumerical characters.

The output for the input of `How are you?` is shown in Figure 1.

2 Submission

1. **Electronic submission** (Due by Wednesday, December 7, 2016 11:59PM)

   (a) Make sure that your program is compilable

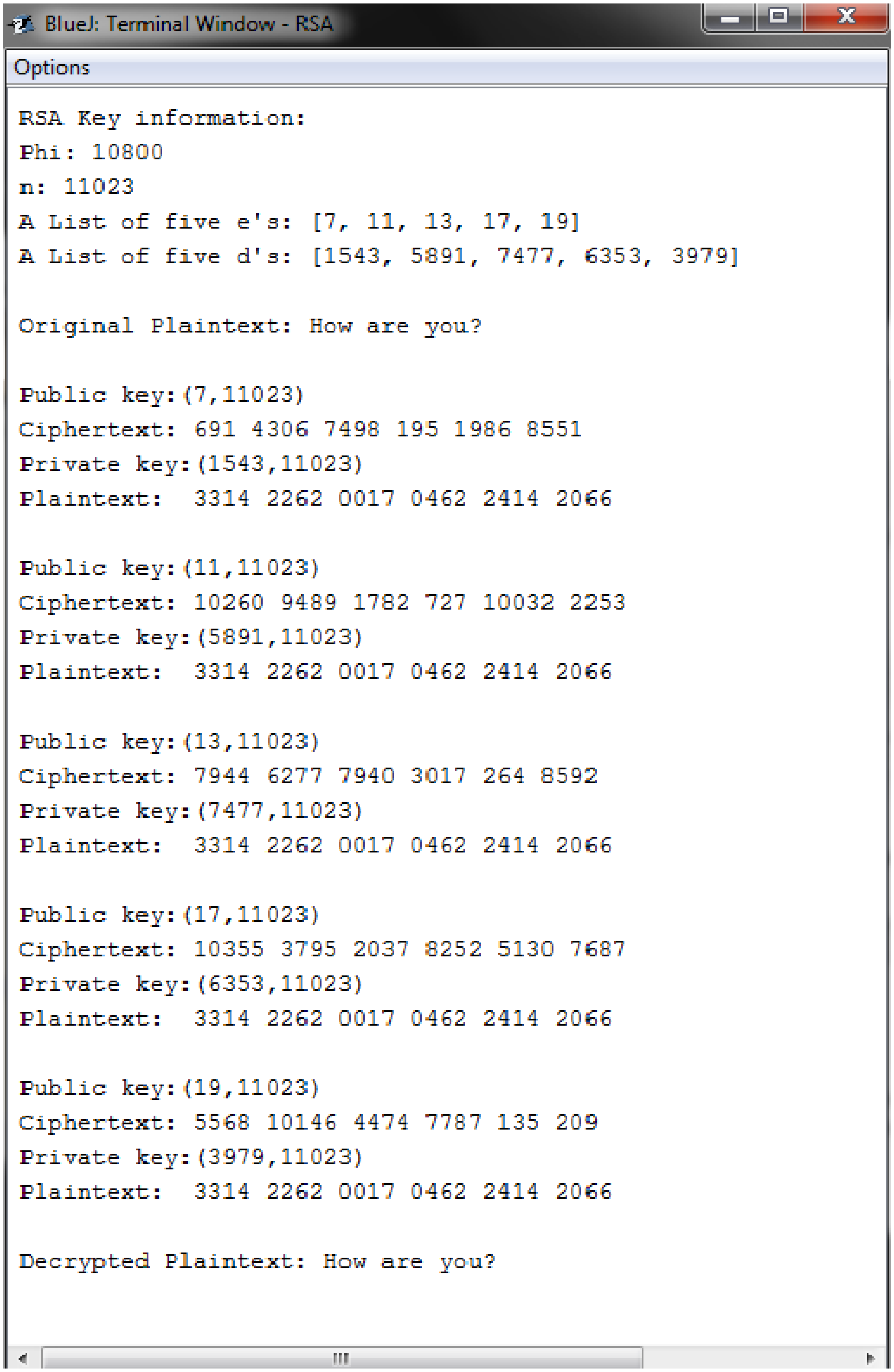
   (b) Zip both the source codes and output screenshots into a file. The file format is as follows: `FirstNameLastName_Program5.zip` (e.g., `DongshengChe_Program5.zip`)

   (c) Upload the zip file onto D2L Dropbox

2. **Hardcopy submission** (Due by Thursday December 8, 2016 in class)

   Your hardcopy should include:

   - Grading sheet (top)
   - Source code (middle)
   - Output screenshots for both plaintexts (bottom)



```
RSA Key information:
Phi: 10800
n: 11023
A List of five e's: [7, 11, 13, 17, 19]
A List of five d's: [1543, 5891, 7477, 6353, 3979]

Original Plaintext: How are you?

Public key:(7,11023)
Ciphertext: 691 4306 7498 195 1986 8551
Private key:(1543,11023)
Plaintext:  3314 2262 0017 0462 2414 2066

Public key:(11,11023)
Ciphertext: 10260 9489 1782 727 10032 2253
Private key:(5891,11023)
Plaintext:  3314 2262 0017 0462 2414 2066

Public key:(13,11023)
Ciphertext: 7944 6277 7940 3017 264 8592
Private key:(7477,11023)
Plaintext:  3314 2262 0017 0462 2414 2066

Public key:(17,11023)
Ciphertext: 10355 3795 2037 8252 5130 7687
Private key:(6353,11023)
Plaintext:  3314 2262 0017 0462 2414 2066

Public key:(19,11023)
Ciphertext: 5568 10146 4474 7787 135 209
Private key:(3979,11023)
Plaintext:  3314 2262 0017 0462 2414 2066

Decrypted Plaintext: How are you?
```

Figure 1: A sample screenshot of outputs