Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Algorythmique et structure de données

T1A

Réseau et Sécurité

S10 Cryptographie et RSA

Roten Marc

2017/2018

Table des matières

Chapitre 1

Exercices

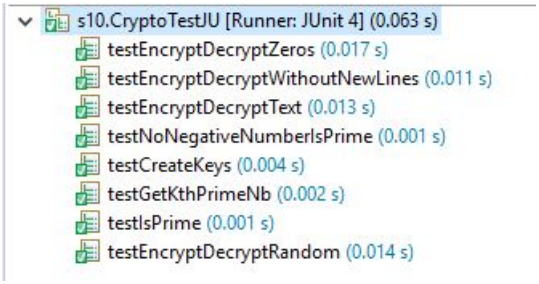
1.1 Ex 1

1.1.1 Code Crypto

```
public static void decrypt(String msgFile, String keyFile,
   String outFile)
                    throws IOException {
  BufferedReader fm = new BufferedReader(new
     FileReader(msgFile));
  BufferedReader fk = new BufferedReader(new
     FileReader(keyFile));
  PrintWriter fo = new PrintWriter (new FileWriter(outFile));

  long e = Long.parseLong(fk.readLine());
  long n = Long.parseLong(fk.readLine());
  fk.close();

  String s = fm.readLine();
  while(s!= null){
    long m = Long.parseLong(s);
    fo.print(decode(m,e,n));
    s = fm.readLine();
  }

  fm.close();
  fo.close();
}
// ------------------------------------------------------------
// public key file : line 1 : number e
//                   line 2 : number N
// private key file : line 1 : number d
//                   line 2 : number N
```

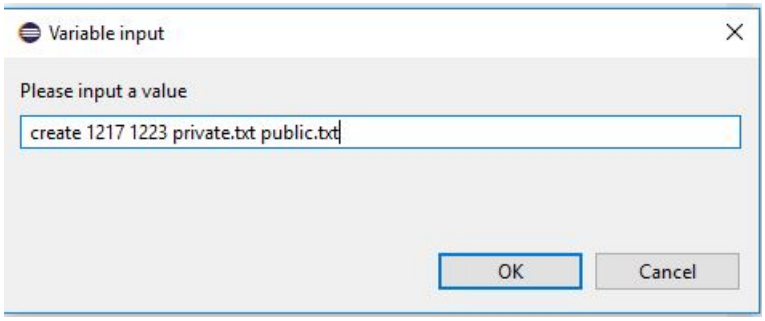
```
// code1-2 :    indices of the desired prime numbers for p and
   q
//              (here e is chosen non-randomly)
public static void createKeys(int code1, int code2,
                String publicKeyFile,
                String privateKeyFile ) throws IOException {
  long p = getKthPrimeNb(code1);
  long q = getKthPrimeNb(code2);
  long n = p*q;
  long nPrime = (p-1)*(q-1);
  long e = getRelativePrime(nPrime);
  long d = multInverse(e, nPrime);
  PrintWriter fa = new PrintWriter (new
     FileWriter(publicKeyFile));
  PrintWriter fb = new PrintWriter (new
     FileWriter(privateKeyFile));
  System.out.println("p="+p+",q="+q+",e="+e+",n="+n+",nPrime="+nPrime
              +",d="+d);
  fa.println(e); fa.println(n); fa.close();
  fb.println(d); fb.println(n); fb.close();
}
// -------------------------------------------------------------
public static boolean isPrime(long n) {
 if(n<=1){return false;}
  for(long i = 2; i <= Math.sqrt(n); i++)
  {
    if(n%i == 0){return false;}
  }
  return true;
}
// -------------------------------------------------------------
// PRE: kth > 0
public static long getKthPrimeNb(int kth) {
  int k = 0, n= 0;
  while(k != kth){
    if(isPrime(n)){k++;}
    n++;
  }
  return n-1;
}
```

1.1.2 Code JUnit

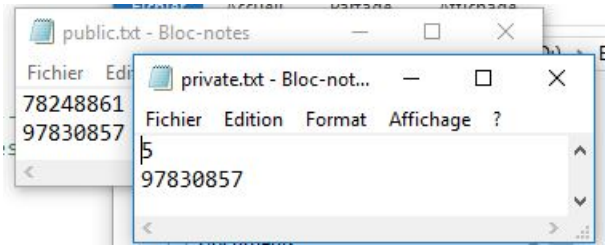


1.1.3 Encryptage

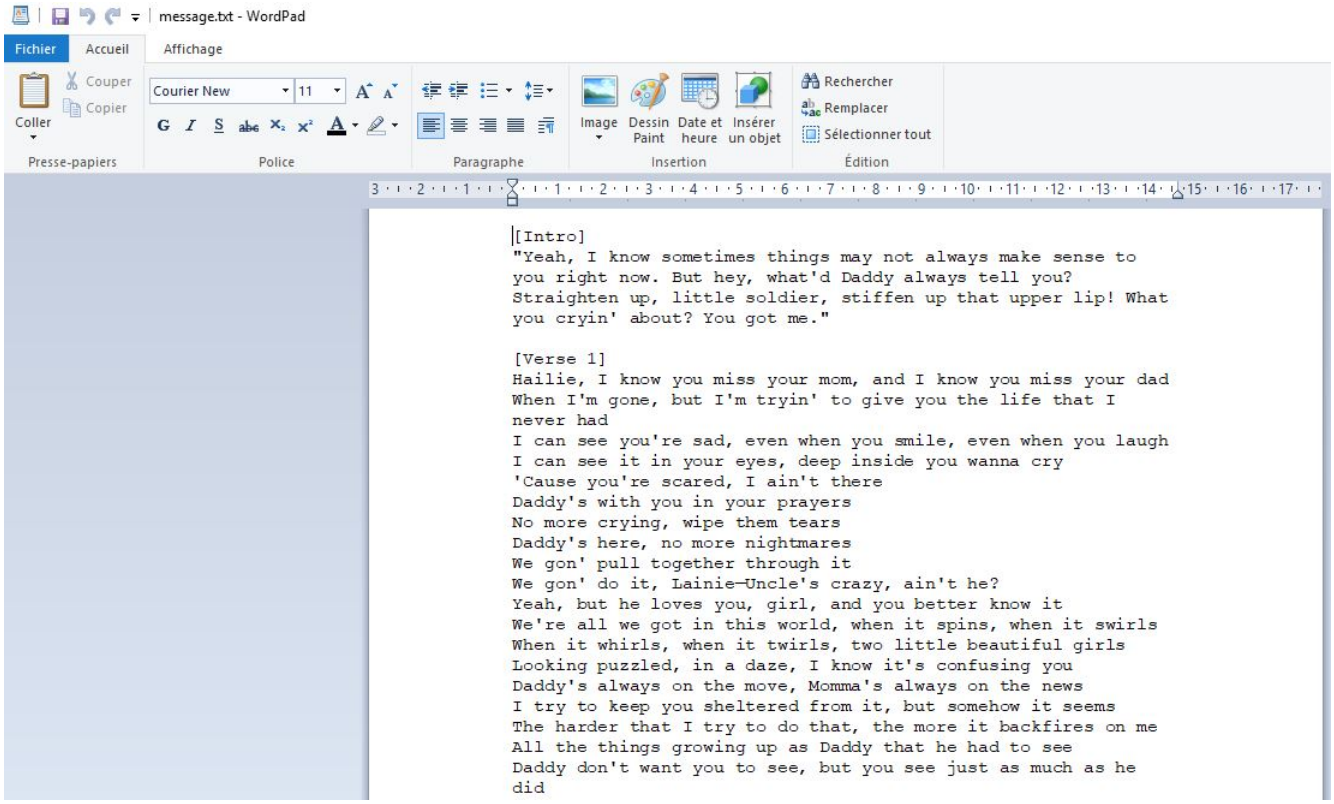
Nous allons tout d'abord créer nos clés privées et publiques



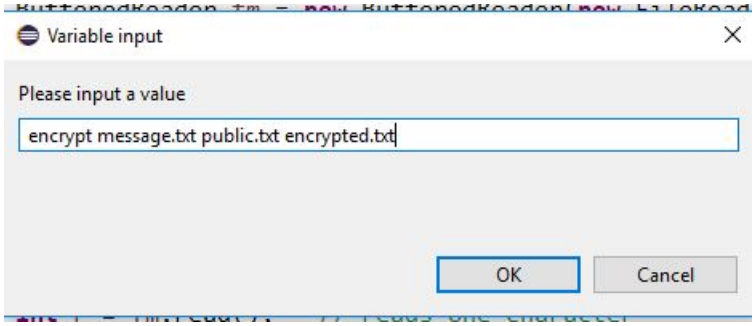
Voici les clés crées



Encryptons maintenant notre message



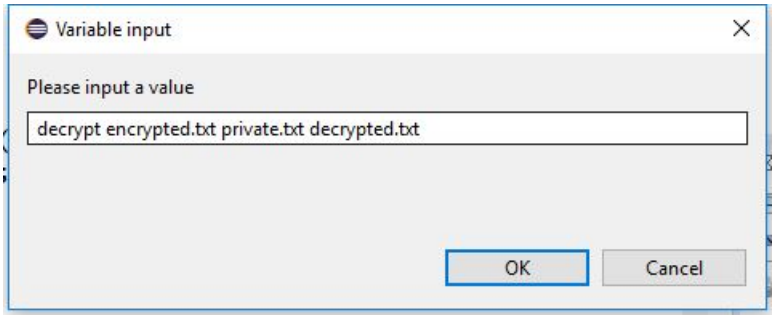
avec la fonction suivante



le résultat est le suivant

```
20871067 26657151 2        86446805 89452930
34336804 89334870 55753514 2        43356897
43356897 2        67409099 25641314 89334870
26657151 85739181 83938333 89334870 36698282
66307825 89334870 2        55753514 2
89334870 55753514 89704590 2        85739181
8818636  2        64970801 73183834 89334870
18833892 66307825 26657151 89334870 55753514
45246613 64970801 26657151 26657151 2
26880344 73183834 89704590 2        64204473
25641314 46899824 94654999 64204473 64970801
94654999 26657151 2        94654999 94808310
31961267 2        94808310 2081445  94808310
46899824 43356897 89334870 26880344 2
83938333 89334870 89704590 18833892 85739181
2        36698282 26424124 45246613 89334870
34336804 2081445  64970801 18833892 55753514
2        2        94654999 45246613 66307825
89452930 5994781  66307825 20871067 2
43356897 55753514 83938333 67995165 26424124
89334870 26657151 2        94654999 31961267
36698282 2        94808310 66307825 26424124
2        46899824 26657151 94808310 18833892
94808310 94654999 64970801 94654999 45246613
89334870 85739181 4248013  2        5993872
64204473 83938333 4248013  52138093 46899824
94654999 2        94654999 8818636  94654999
26657151 36698282 43356897 18833892 43356897
64970801 46899824 2        45246613 2
64204473 31961267 55753514 38038532 34336804
94654999 26657151 67409099 31961267 85758340
94808310 85758340 2        64970801 64204473
2        26424124 26657151 89704590 2        ..... ainsi de suite
26657151 2        46899824 64970801 73183834
46899824 21232105 31961267 94654999 89334870
64970801 31961267 26657151 83938333 43356897
43356897 26424124 2        2        94654999
73183834 26424124 55753514 34336804 83938333
94808310 85739181 67409099 2        2
2        2        67409099 39452930 6169242
64204473 31961267 94654999 43356897 55753514
31961267 89704590 66307825 89334870 26657151
85739181 36698282 2        36698282 2
2        31961267 89704590 2        34336804
43356897 85739181 64970801 85739181 85758340
89334870 94808310 67409099 89334870 64204473
26657151 2        55248633 55753514 2
2        26657151 2        2        26657151
31961267 94654999 5993872  64204473 66307825
89704590 89704590 46899824 64970801 85739181
36698282 89704590 31961267 94808310 64970801
31961267 2        26657151 2        85758340
85739181 85739181 2        85739181 2
94808310 89334870 85739181 89334870 26657151
2        55753514 89334870 55753514 89334870
64204473 86446805 55753514 66307825 2
31961267 2        2        2        73183834
39452930 47975402 78114210 64204473 64970801
94654999 26657151 66307825 89334870 47832210
2        66307825 85739181 64204473 94654999
94808310 31961267 64970801 83938333 2
94654999 64970801 43356897 2        85739181
43356897 73183834 85758340 31961267 89334870
94808310 46899824 2        43356897 55753514
94654999 26657151 31961267 26424124 2
2        94654999 6169242  2        26657151
26657151 43356897 89334870 34336804 46899824
89334870          55753514 2        94654999
                  26657151
```

Décryptons ce message



Le résultat décrypté donne

decrypted.txt - Bloc-notes

Fichier Edition Format Affichage ?

[Intro]
"Yeah, I know sometimes things may not always make sense to you right now. But hey, what'd Daddy always tell you? Straighten up, little soldier, stiffen up that upper lip! Wh

[Verse 1]
Hailie, I know you miss your mom, and I know you miss your dad
When I'm gone, but I'm tryin' to give you the life that I never had
I can see you're sad, even when you smile, even when you laugh
I can see it in your eyes, deep inside you wanna cry
'Cause you're scared, I ain't there
Daddy's with you in your prayers
No more crying, wipe them tears
Daddy's here, no more nightmares
We gon' pull together through it
We gon' do it, Lainie—Uncle's crazy, ain't he?
Yeah, but he loves you, girl, and you better know it
We're all we got in this world, when it spins, when it swirls
When it whirls, when it twirls, two little beautiful girls
Looking puzzled, in a daze, I know it's confusing you
Daddy's always on the move, Momma's always on the news
I try to keep you sheltered from it, but somehow it seems
The harder that I try to do that, the more it backfires on me
All the things growing up as Daddy that he had to see
Daddy don't want you to see, but you see just as much as he did
We did not plan it to be this way, your mother and me
But things have got so bad between us, I don't see us ever being
Together ever again, like we used to be when we was teenagers
But then, of course, everything always happens for a reason
I guess it was never meant to be, but it's just something
We have no control over, and that's what destiny is
But no more worries, rest your head and go to sleep
Maybe one day we'll wake up and this'll all just be a dream

[Hook]
Now hush, little baby, don't you cry
Everything's gonna be alright
Stiffen that upper lip up, little lady, I told ya
Daddy's here to hold ya through the night
I know Mommy's not here right now, and we don't know why
We fear how we feel inside
It may seem a little crazy, pretty baby
But I promise, Momma's gon' be alright
(Heh, it's funny)

[Verse 2]
I remember back one year when Daddy had no money
Mommy wrapped the Christmas presents up and stuck 'em under the tree
And said some of 'em were from me 'cause Daddy couldn't buy 'em
I'll never forget that Christmas, I sat up the whole night cryin'
'Cause Daddy felt like a bum—see, Daddy had a job
But his job was to keep the food on the table for you and Mom
And at the time, every house that we lived in
Either kept gettin' broken into and robbed or shot up on the block
And your mom was saving money for you in a jar
Tryin' to start a piggy bank for you so you could go to college