Durham University
School of Engineering and Computing Sciences

Software Methodologies - Digital Communication

Summative Assignment

Coursework description

This assignment involves creating simple programs (written in Python or Java) to compute encryptions, decryptions and signatures. You should then use your code to answer the following questions. You should submit your source code and a PDF containing the answers to the questions. **I am only intending to mark the pdf file:** the marks are allocated for the answers to questions, but the source code is also handed in so that we can verify where the answers came from if necessary and that it is your own work. Submit the source code and PDF of answers electronically via DUO.

Programming Objectives

You will need two programs in order to answer the questions below: one to encode and decode a Vigenere cipher, and another to encode and decode using RSA.

Vigenere cipher:

- Your program should be able to take messages, ciphertexts and keys consisting of English uppercase letters only.
- The encoder should take two parameters: a message and a key.
- It should extend the key to the length of the message by repeating it as required, and at each position in the message add the letter values together (mod 26) to obtain the encryption.
- Decryption should be implemented to correctly decrypt.
- Test case:

Message:	`BLACKBEARDISSAILINGTOJAMAICA`
Key:	`YOHOHO`
Ciphertext:	`ZZHQRPCOYRPGQOPZPBEHVXHAYWJO`

RSA calculations:

- Your program should be able to efficiently compute x^y mod n (that is x to the power y modulo n).
- It should use only basic functions (multiplication, taking the remainder in a division, modulo operator, etc.), not specialist BigInteger or Power functions.
- It should be able to handle x,y,n being ints, i.e. having values between 0 and 2,147,483,647.
- It should be able to output each intermediate value calculated, as well as the final answer. For each intermediate value it should state what it is as well as its value, e.g. if your code was given the task 45^{67} mod 23, and calculated 45^3 along the way, it might output “45^3 = 22 mod 23” as part of its working.

continued on next page

Questions

1. Give the encryption of LETSSAILFORTHESPANISHMAIN using the Vigenere cipher and key PIECESOFEIGHT

   5 marks

2. Give the decryption of ZVTVKGVBLNWYJVCLBOOHSSKFIGWYOEDNZ using the Vigenere cipher and key GOLDCOINS

   5 marks

3. Alice and Bob decide to use a One Time pad, based upon the Vignere cipher, to encrypt messages between themselves. However they have not previously arranged a key. They decide to each generate their own keys: K_A and K_B. Then:
   3.1. Alice will generate the message, encrypt it with K_A to obtain C_1, and send it to Bob.
   3.2. Bob will re-encrypt it with K_B, obtaining C_2, and send it back to Alice.
   3.3. Alice will decrypt C_2 using K_A, and send the result, C_3, back to Bob.
   3.4. Bob will decrypt C_3 using K_B, and recover the original message.

   You intercept the transmissions:
   C1 =

   ```
   KPKWETQKAODLZMERBOCAPNEERINWHQYBUOQUWTXMKIIBLNISOQAFRQHFHBE
   YXUPDMIMHEJNURXYQCXMULOVEKKXZZQWUUIBVSLMDJYQGBEVBIXDSJVXVPM
   YAAZROGEBGWIEVHLADXKRUIUYZDNCJTTKXDCHKNWGDNCKQGCBZVZNJPOFDY
   WWYRDMKFHKXFMFRGLMKHRWHFRJVNSGAQJHNCBYGSCEOPDVRRPPFWLOGUSRH
   ZRIIAKYGZBJVPPQLRMMFGFBXTSMBJFLBOAWBKCD
   ```

   C2 =

   ```
   IXYVAGYZLHMRCLAGUGXEQSMFXAZTHFCKNSGXINVHWDOOUPVUNYIZFMKYTOV
   KKEADYZPZGXWJFVSXGMXAZMHQTRPYGIXTESRVIGWWSLTHXIZIDPEVSSDRHI
   KKGDTYHWICSYTOIWPUBZNFVEZCHWWGHUAJBBXIJTGLRJHGLHXRNJANPNPZW
   ZYCIPHPYOANIPHOBKKRPYJHVTTEHROJYQCDTRDOWUKGCEEPLVNZSRCMTOUY
   LHWNHXGHNMWJEMHCIOHKNIHXSOTMDRSCBQYZYNU
   ```

   C3 =

   ```
   YAGNKAIHHXBZDQPTWHMSHWINSAZDWTJXNRTWAISMEPXCAKFGSPINWPZTEAK
   MFOLSKKRYGHYGCELHQHCOUFFMBDWGHVUGYEWHJYOUDTJJJKLHYLPENAOOUK
   HOXIFSDSUNACTFCPGKLTAINMULRBNXBUMTCMYPAXLQDLAJMFPSDKEKEOKNR
   RHQPXDKXMHEPWJBINLDIZTOYPQCIAMBXLIJZDKQRVOFTNRQNGIYOOBSXKZE
   BHCLYNUTALHFXZVNZNFJZGOSBKCPLEKFOKIEWYX
   ```

   What was the original message?

   10 marks

4. Use your code to compute each of the following values, showing all intermediate terms computed:
   (i) 17^{54} mod 139 **2 marks**
   (ii) 2345^{65531} mod 265189 **3 marks**
   (iii) 4733459^{65537} mod 75968647 **5 marks**

Continued on next page.

In the questions below, the bank's RSA public key is (76282747,65537); your own public key is (9436709, 1676267) and your private key is d=3497603.

5. You wish to securely send the message M=654733 to the bank.
   (i) State the calculation to encrypt this message for sending to the bank. **5 marks**
   (ii) State the encrypted value, calculated using your code. **5 marks**

6. The bank sends you an encrypted message 1684446.
   (i) State the calculation used in decryption. **5 marks**
   (ii) What is the decrypted value in this case? **5 marks**

7. The bank requests a signed encrypted message from you so that they can verify that you are the sender and the message is secure in transmission to them. You should encrypt the message and signature as two separate blocks. They already know your public key.
   (i) State the calculation to sign and encrypt the message 337722. **10 marks**
   (ii) What is the transmission made for the message 337722 when it has been signed and encrypted? **10 marks**

8. They return the following signed and encrypted message to you:
   (C(M),C(S)) = (4647068,526345).
   (i) State the calculations required to decrypt and verify the message. **3 marks**
   (ii) State the values in this case. **5 marks**
   (iii) State whether the signature is valid or not. **2 marks**

9. You wish to demonstrate to the bank that you know a third party (Bob), by showing a signed message that appears to come from Bob. Bob's public key is (122269479,53407), but you do not know his private key. Construct a valid singed message from Bob, and show that the check calculations confirm that signature is valid.
   10 marks

10. You intercept a message from Bob to the bank, which says: "My new 3-digit PIN code is in the encrypted attachment. Yours Bob." and comes with the attachment (58621765). How can you crack such a message and what is Bob's new PIN?
    10 marks

Total: 100 marks