COMP90007 Internet Technologies
Week 12 Workshop

Semester 2, 2019

Suggested solutions

Question 1

Given the RSA algorithm we studied last week, if p = 3, q = 11 and if d = 3 and e = 7 instead of the version we saw in class, using the same character mapping we saw in class though, where A is 01 and B is 02, and C is 03 and so on, how would RSA work? Would it work at all? Show in detail what numbers would be computed and transmitted at both ends of a transmission if we want to send across a "D". Show where it fails if it does not work properly?

Ans: It Works! p = 3, q = 11 means z is (3 - 1) x (11 - 1) = 20

d is chosen to be 3 which has no common factors with z which is good. e is 7 which means (d x e) is 3 x 7 = 21. Thus 21 mod 20 is 1 which is another good choice!

n is p x q = 33

For encryption the pair to use 7,33 which is the public key ,and for decryption 3, 33 is used which is the private key! To send "D", first we see that it has numerical value is 4 as per this question's suggestion. And 4 ^ 7 = 16384

16384 mod 33 = 16 is found next (Ok to use a calculator here but not necessary if you see 4 ^ 7 is 2 ^ 14)

16 is sent in transmission and then we take 16 ^ 3 = 4096 upon receipt, and then 4096 mod 33 to get 4 which concludes decryption, 4 is "D" in our coding. Eureka!

Question 2

Using the RSA algorithm we saw in class, please design a simple algorithm to sign documents where the sender cannot refute the fact that a document was signed by herself later on. Which property of RSA your algorithm relies on?

Ans. The algorithm is as follows:

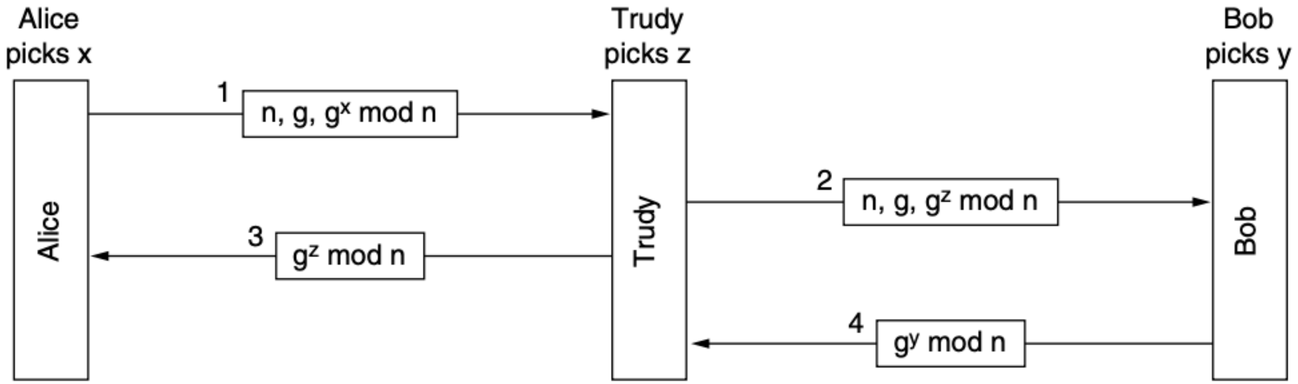
- Someone sends a document for signature to person A.
- Our person A signs it by using her private key PrK to, pretty much uses private key to lock the document.
- Then this message is sent to whoever needs it. We can add the plain text message to this communication as well or the original document can be accessible from a webpage etc.
- Receiver uses the public key of the sender A, say PuK, to open the message and if the text matches the original plaintext of the document then sender A should be the one who signed this document as there is no other person who can lock the document with her private key as only she knows that key; which only our public key is capable of countering the effect of...

We rely on the property that E(D(P)) = P in RSA as well as D(E(P)) = P
using these key pairs.

Question 3

Given the Diffie-Hellman key challenge in the lectures please develop the full flow chart for the man-in-the-middle (MITM) attack, with step numbers and messages sent, show details about how this attack would work.

Ans.



Refer to section 8.7.2 of Tanenbaum.

Question 4

Leveraging the authentication protocol using Public-Key cryptography, we send across two additional numbers, RA and RB. Why are these needed? Why not Alice sends only her name to Bob but needs a RA as well?

Ans. Without RA Bob can still send back an acknowledgement but Alice cannot be sure that whether the responding person is Bob or not. The RA is needed to prove that Bob opened the initial message with his private key, saw RA, and in the response message sends it to Alice to prove this. Same is true for the role of RB.

Question 5

Please list, summarize the four key areas/aspects of network security.

Ans. The four key areas/aspects are:
Secrecy: keeping information hidden from a general audience, i.e., except the intended party

Authentication: Ensuring the user you are giving the content to has the valid id/credentials

Non-repudiation: Proving that the content belongs to/send by a named sender

Integrity control: Ensuring the content is not tampered with, e.g., during transport