COMP90007 Internet Technology

Week12

Yiran (Scott) Ruan

Email: yrrua@unimelb.edu.au

GitHub: https://yiranruan.github.io

Tutor feedback

- Google ’Casmas tutor feedback’
- Choose COMP90007

- Line: https://apps.eng.unimelb.edu.au/casmas/index.php?r=qoct/feedback&subjCode=COMP90007

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?

Process

- C = ciphertext, P = plaintext, E = encryption, D=decryption
- **K1, K2 = keys**
- $C = E_{K1}(P)$

  Sender knows the public key $K1$ and the P
- $P = D_{K2}(C)$

  Only receiver knows private $K2$ which can undo $K1$'s effect
- $D_{K2}(E_{K1}(P)) = P$

  Only way to acquire Plaintext is using K2 to do decryption

Puk & PrK

- Diffe-Hellman key system
- **Key 1: public key**, usable by anyone **to encrypt** messages to the owner of the key, this key known to all
- **Key 2: private key**, required **to decrypt** the message and known only by the owner of this key

RSA

- **RSA - Rivest, Shamir, Adleman**
- Key generation:
  - Choose two large primes, p and q
  - Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$.
  - Choose d to be relatively prime to z, i.e., **no common factors**
  - Find e such that

$$(\boldsymbol{d} \times \boldsymbol{e})\, \boldsymbol{mod}\, \boldsymbol{z} = \mathbf{1}$$

  - Public key is (e, n), and private key is (d, n)

Step by Step

- Choose two large primes, p and q

$$p = 3$$
$$q = 11$$

- Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$.

$$n = 3 \times 11 = 33$$
$$z = (3 - 1) \times (11 - 1) = 20$$

Step by Step

- Choose d to be relatively prime to z, i.e., **no common factors**

$$d = 3$$

- Find e such that

$$\boldsymbol{(d \times e)\ mod\ z\ =\ 1}$$

Step by Step

- Choose d to be relatively prime to z, i.e., **no common factors**

$$d = 3$$

- Find e such that

$$\boldsymbol{(d \times e)\ mod\ z\ =\ 1}$$

==> $\boldsymbol{(3 \times e)\ mod\ 20\ =\ 1}$

==> $\boldsymbol{e\ =\ 7}$

- So we get the public key and private key:

Public key: (e, n) -> (7, 33)

Private key: (d, n) -> (3, 33)

Step by Step

- Encryption:

$$Cipher \ = \ Plain^{e}(mod\ n)$$

- Decryption:

$$Plain \ = \ Cipher^{d}(mod\ n)$$

- Let’s encode and decode an example. How about ‘D’……

Encryption

- Encryption:

$$Cipher \ = \ Plain^{e}(mod\ n)$$

- ‘D’ is mapping to 4
- So…

$$Cipher \ = \ 4^{7}(mod\ 33) = 16$$

Decryption

- Decryption:

$$Plain\ =\ Cipher^{d}(mod\ n)$$

- The code that we have received is ‘16’.
- So…

$$Plain\ =\ 16^{3}(mod\ 33) = 4$$

- 4 is mapping to ’D’ and we decode the message successfully.

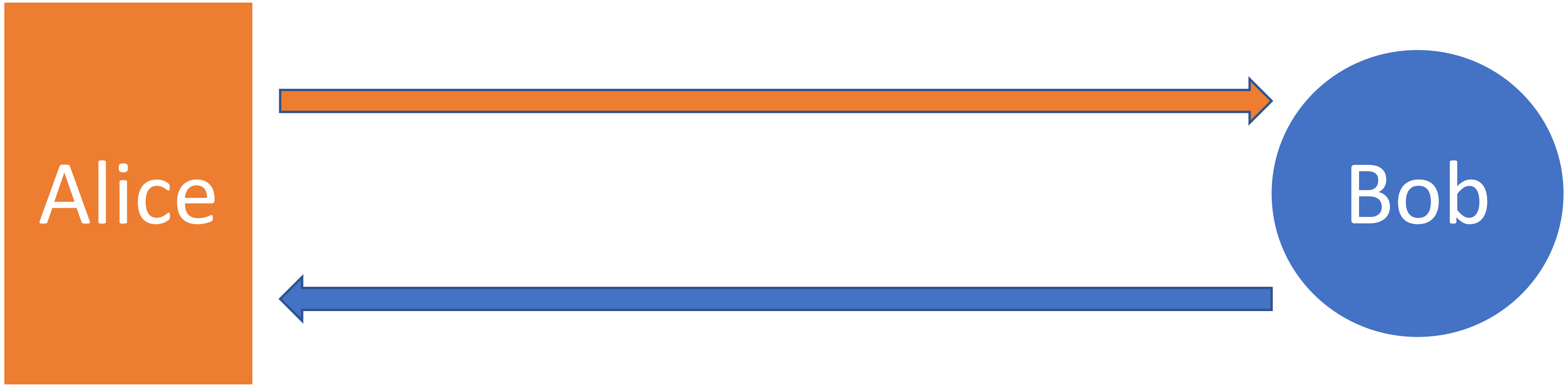
Solution 1

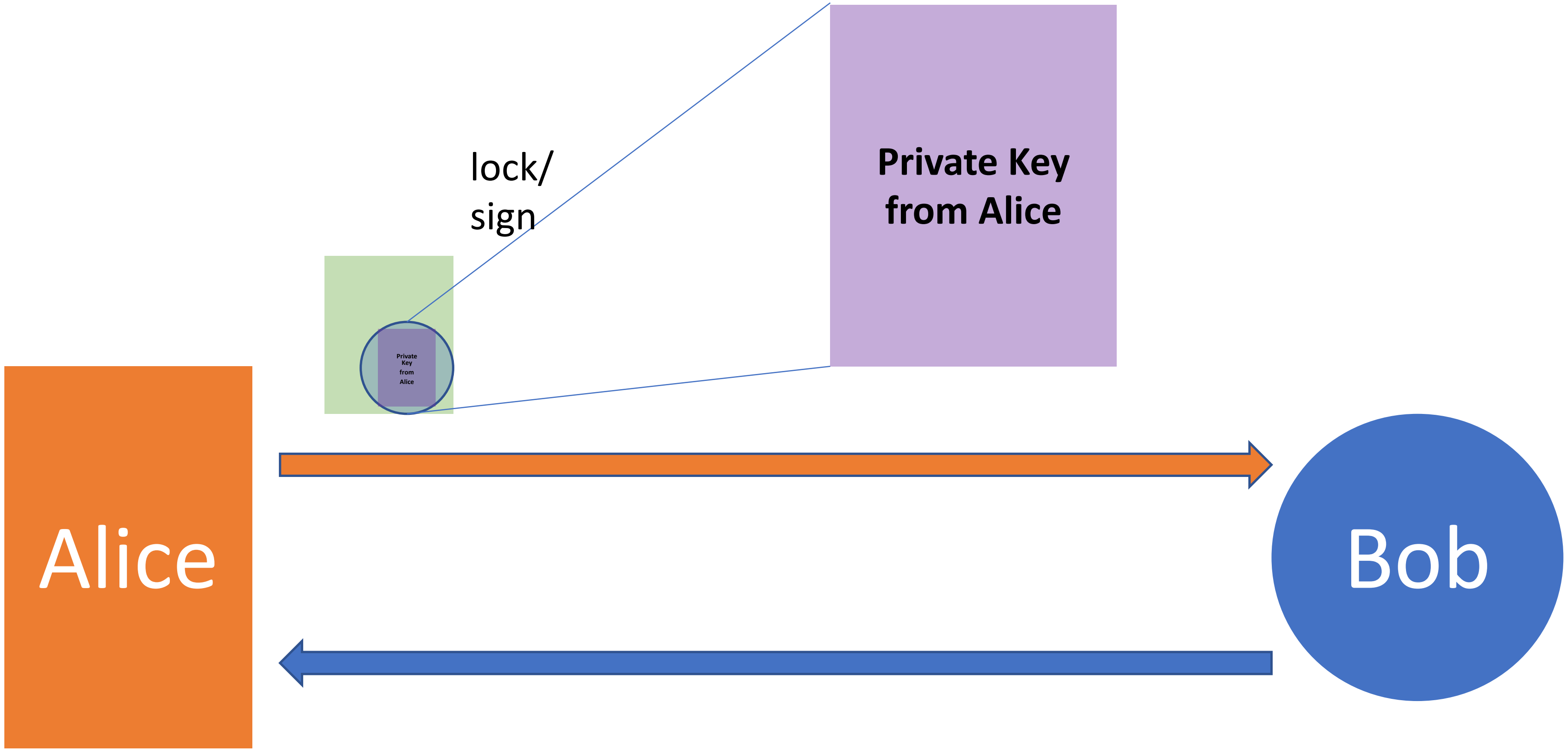
- It Works! Please refer to Week11 Lecture2 slides 4 and 6. p=3, q=11 means z is (3-1)x(11-1)=20
- d is chosen to be 3 which has no common factors with z which is good. e is 7 which means (d x e) is 3 x 7 = 21. Thus 21 mod 20 is 1 which is another good choice!
- n is p x q = 33
- For encryption the pair 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?

Alice have to include some info which is only known by herself but not any one else.





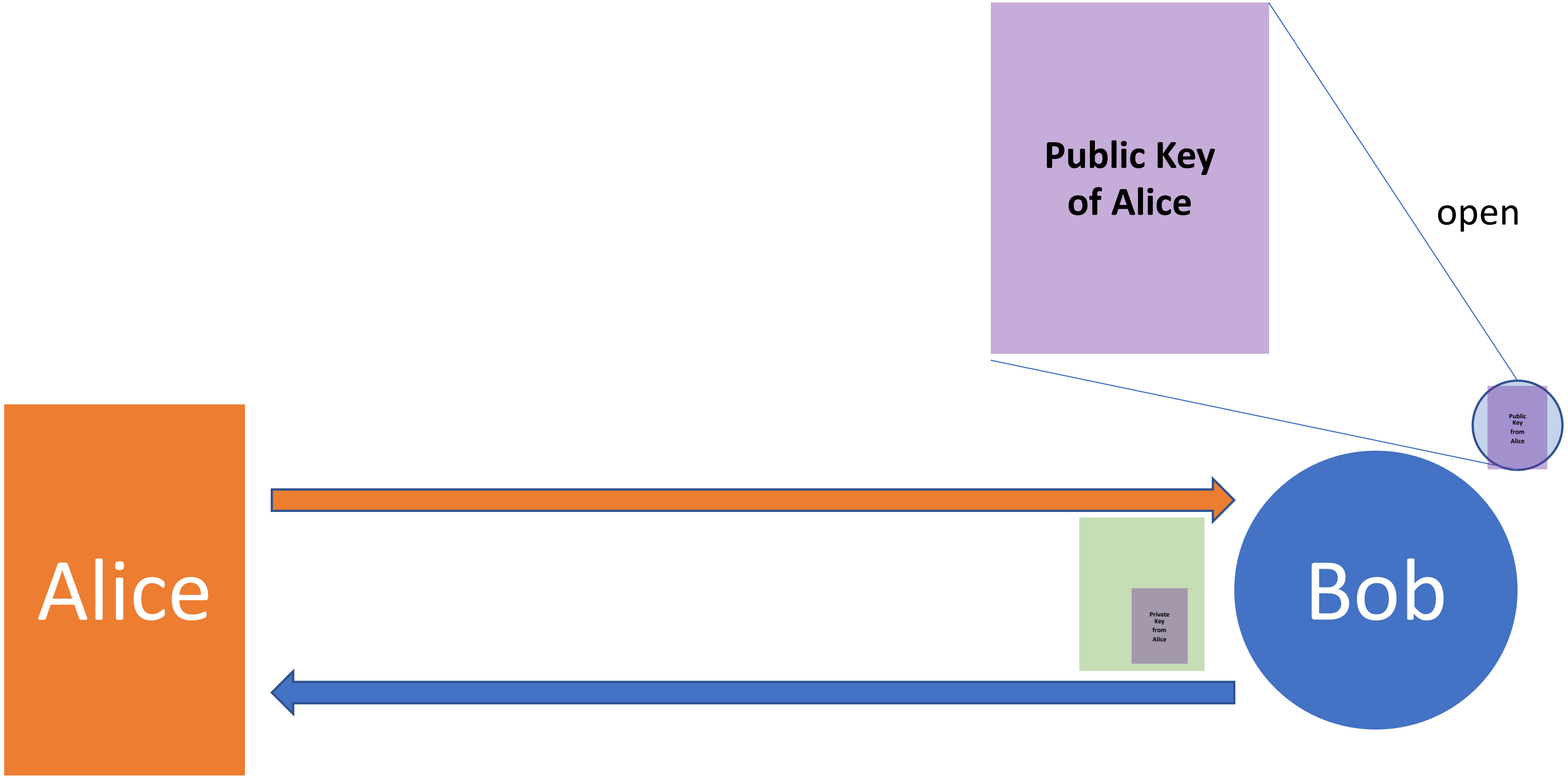
lock/
sign

Private Key
from Alice

Private Key from Alice

Alice

Bob



Public Key of Alice

open

Public Key from Alice

Alice

Private Key from Alice

Bob

Solution 2

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 lecture 3 for week 11 slide 3. 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.

Diffie-Hellman key exchange

- **Diffie-Hellman key exchange** allows strangers to establish a shared secret key.
- Step 1. Alice and Bob have to agree on two large numbers, n and g.

  -> n is a prime and $(n-1)/2$ is a prime and certain conditions apply to g
- Step 2. Then Alice picks a large (say, 1024-bit) number, x, and keeps it **secret**. Similarly, Bob picks a large secret number, y.

Diffie-Hellman key exchange

- Initiates the key exchange protocol:

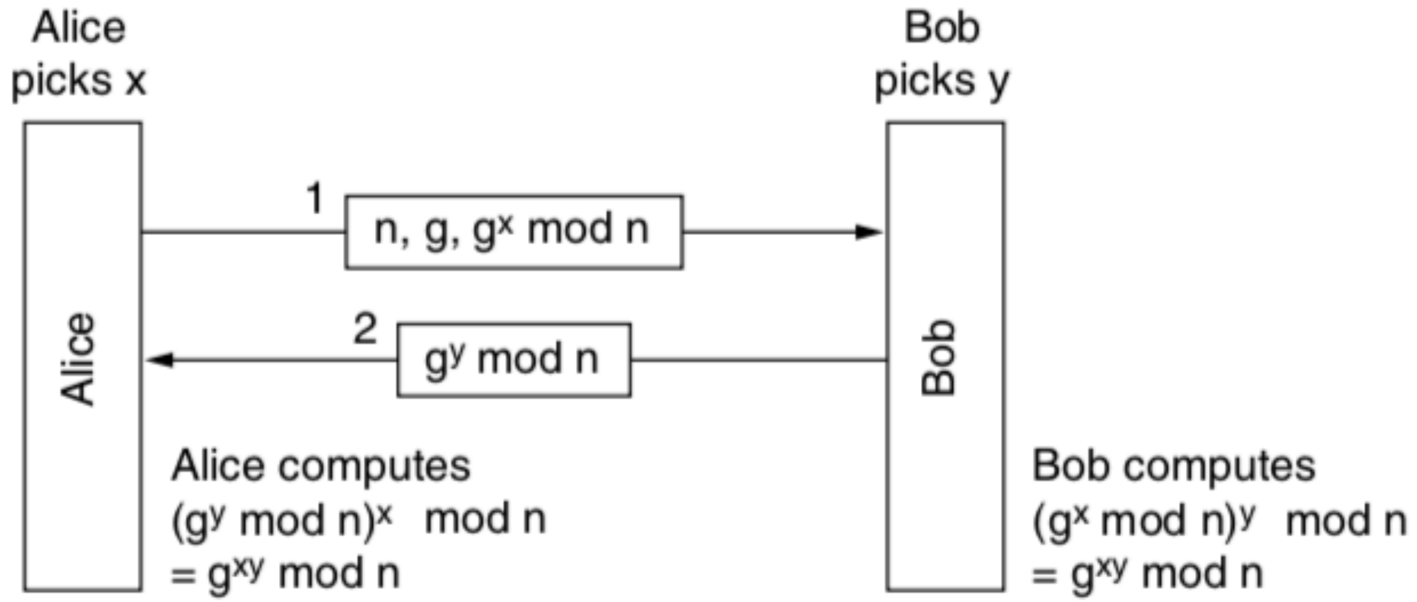


Figure 8-37. The Diffie-Hellman key exchange.

Diffie-Hellman key exchange

- If we said, another person, Trudy, has seen both messages.
- If she could compute *x* and *y*, she could figure out the secret key.
- However, given only $g^x \ mod \ n$, she cannot find x.
- It seems like a impossible work to hack the messages….
- Is that true?

Man-in-the-middle attack

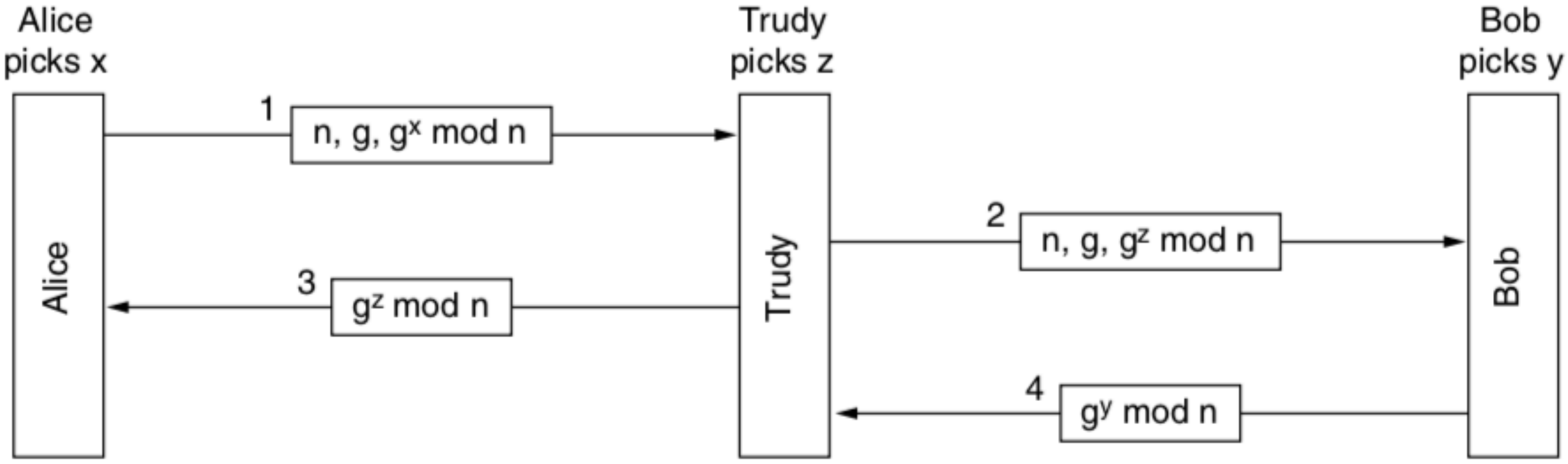


Figure 8-38. The man-in-the-middle attack.

Man-in-the-middle attack

- Alice thinks she is talking to Bob, so she establishes a session key (with Trudy). So does Bob.
- Every message that Alice sends on the encrypted session is captured by Trudy, stored, modified if desired, and then (optionally) passed on to Bob. Similarly, in the other direction, Trudy sees everything and can modify all messages at will, while both Alice and Bob are under the illusion that they have a secure channel to one another.

Solution 3

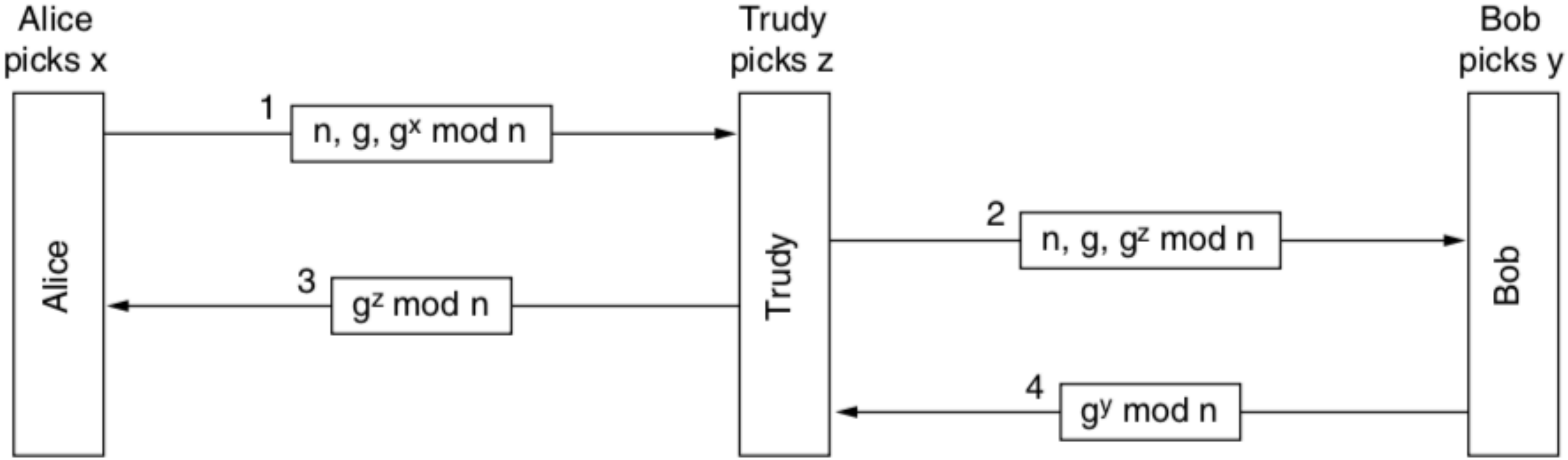
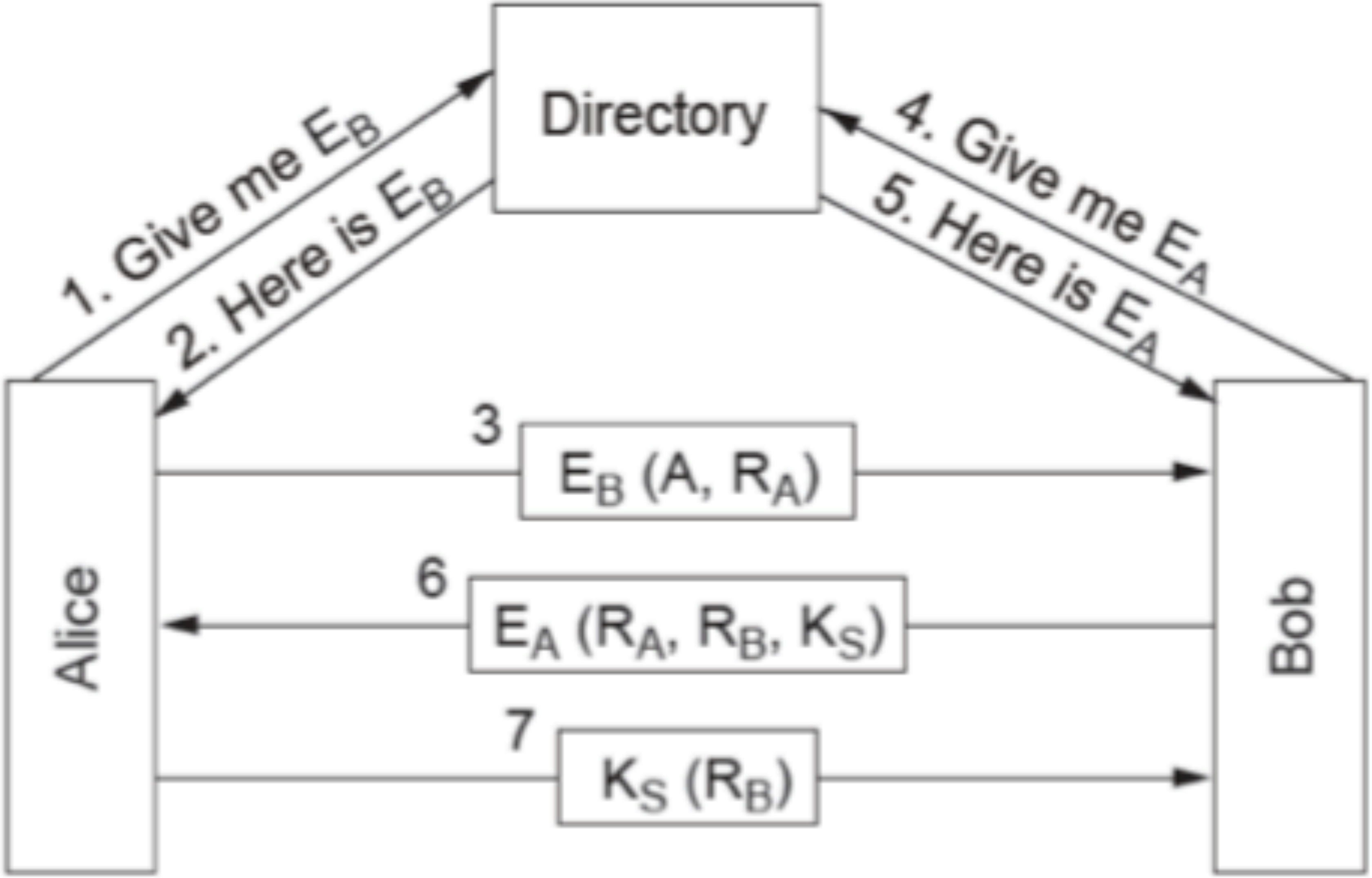


Figure 8-38. The man-in-the-middle attack.

- Refer to section 8.7.2 of Tanenbaum.

Question 4

- Leveraging the authentication protocol using Public-Key cryptography (Lecture 3, week 11, slide 6), 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?


Directory
1. Give me E_B
2. Here is E_B
4. Give me E_A
5. Here is E_A
Alice
Bob
3
E_B (A, R_A)
6
E_A (R_A, R_B, K_S)
7
K_S (R_B)

Solution 4

- 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.

Network security

- **Secrecy**, also called confidentiality, has to do with keeping information out of the grubby little hands of unauthorized users. This is what usually comes to mind when people think about network security.
- **Authentication** deals with determining whom you are talking to before revealing sensitive information or entering into a business deal.

Network security

- **Non-repudiation** deals with signatures: how do you prove that your customer really placed an electronic order for ten million left-handed doohickeys at 89 cents each when he later claims the price was 69 cents? Or maybe he claims he never placed any order.
- **Integrity control** has to do with how you can be sure that a message you received was really the one sent and not something that a malicious adversary modified in transit or concocted.

Solution 5

- 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