Exercises

Introduction - Crypto

Computer Security

Question 0

Consider the phenomenon of identity stealing in social networks (e.g., Facebook, Twitter), which happens when a cyber criminal steals the username and password of a user and uses them to impersonate that user (e.g., post content, send messages to friends, etc., without the user's consent).

What is the risk component in this scenario?

What is the threat/risk component in this scenario?

The risk is that the victim's identity could be used to negatively affect the reputation of the user. Another risk is that the stolen account is used to post malicious content (e.g., links to malicious sites), which is spread among the victim's friends. Further exacerbating the risk is the fact that the user may be using the same password for multiple websites.

What are the assets?

What are the assets?

In the risk scenarios described in the previous answer, one asset is the victim's reputation, another asset is the victim's friends computers.

What is the threat agent?

What is the threat agent?

The threat is a cyber criminal motivated either by hatred against the victim, or by the possibility of abusing the victim's credibility to spread malicious content.

Why is this scenario possible , and how would you mitigate it?

Why is this scenario possible , and how would you mitigate it?

There is no strong authentication mechanism: if the credentials get stolen, there is no assurance on who is using them. A viable solution would be to use a second factor of authentication, such as a token sent via SMS.

Question 1

Consider the following scenario: *A small manufacturing company, one of the most important producers of a specialized musical instrument, is hit by a ransomware attack (i.e., infected by malware with the sole purpose to encrypt all the files in the infected computer until the victim pays a ransom to the attacker). The ransomware is able to quickly propagate to all the computers in use by the company.*

1. What are the <u>two most important Threat/Risk</u> in this scenario? Name and describe each of them, specifying the <u>asset</u> at risk and list one or two possible <u>countermeasures</u>.

Threat/Risk 1 Description:

Asset at risk:

Countermeasure:

Threat/Risk 2 Description:

Asset at risk:

Countermeasure:

Threat/Risk 1 Description: *Loss of business-critical data (e.g., key intellectual property) so that the company is not able to produce the (specialized) goods anymore*

Asset at risk: *Business-critical data*

Countermeasure: *Backups*

Threat/Risk 2 Description: *Loss of production time due to the downtime incurred to restore the infected computers and systems. During this time the factory must me kept shut off, bringing a substantial economic damage.*

Asset at risk: *company's production*

Countermeasure: *redundant systems, isolated systems, procedures for a fast disaster recovery, …*

2. What is (or are) the possible threat agent(s) according to what you answered in (1.)?

2. What is (or are) the possible threat agent(s) according to what you answered in (1.)?

The most likely threat agent is a cybercriminal motivated by the fact that the victim will pay a ransom, due to the value of the assets at risk. Another possible threat agent is a competitor who wants to damage the company's ability to carry on business or to cause monetary loss. If the victim is listed on the stock market a threat agent could be a malicious trader willing to capitalize on stock loss.

Question 2

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

1. [3 points] What are the three most valuable assets at risk in this scenario?

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

1. [3 points] What are the three most valuable assets at risk in this scenario?

- people inside the car
- people outside the car
- car

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

2. [2 points] Suggest at least two potential attack surfaces on the vehicles.

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

2. [2 points] Suggest at least two potential attack surfaces on the vehicles.

- CAN bus via diagnostic port
- Remote interface to car

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

3. [2 points] Suggest, in a rough order of prevalence (i.e., frequency) the two most likely potential digital attacks against such vehicles and their operating companies.

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

3. [2 points] Suggest, in a rough order of prevalence (i.e., frequency) the two most likely potential digital attacks against such vehicles and their operating companies.

- Local: an attacker inside the car can manipulate the packet transiting on the CAN bus via diagnostic port and take control of the car
- Remote: an attacker could manipulate the communication between car and the backend, potentially drive the car somewhere else

Question 3

An Internet-connected “smart speaker”, featuring a voice-controlled intelligent virtual assistant (think about a device similar to Amazon Echo, Google Home, or Jarvis), is installed inside a house.

The speaker is *connected to a wireless network*, and *linked to a cloud service account* (e.g., the owner’s Google/Amazon/iCloud/… account). The device is *always listening for a particular keyword* (e.g., “*OK, Google!*”). As soon as the keyword is detected, it records a short audio clip, which is uploaded to a cloud speech recognition service. Then, the device performs the action requested in the recognized command.

The available actions allow to *search particular pieces of information on the Internet* (e.g., providing weather or traffic information), or to *interact with the owner’s cloud account* (e.g., making and accessing to-do lists stored in the cloud, playing music from a streaming service). Furthermore, the device can act as a *“home automation hub” controlling “smart” devices* via voice commands. Thus, the device supports commands to turn on and off the house lights, open the front door, control the heating, and so on.

1. What are the three most valuable assets at risk in this scenario?

1. What are the three most valuable assets at risk in this scenario?

1) *Personal information (musical preferences, location - e.g., from weather requests, …)*
2) *Owners' voice (recorded commands and the possibility of recording unwanted conversation given that the device sports an always-listening microphone)*
3) *The actual house (remotely-controlled door)*
4) *The device vendor reputation*

2. Suggest at least two potential attack surfaces of this “smart speaker”.

2. Suggest at least two potential attack surfaces of this “smart speaker”.

1) *The voice command interface*
2) *Cloud backend (exploit \ data breaches)*
3) *Local network*
4) *Physical access*

3. Suggest, in a rough order of prevalence (i.e., frequency) the two most likely potential digital attacks in this scenario.

3. Suggest, in a rough order of prevalence (i.e., frequency) the two most likely potential digital attacks in this scenario.

1) *Compromise the cloud vendor to access all the recordings, user data, …, and, according to the implementation, gain control of the house.*
2) *Malicious voice commands: performed by a physical person or even by a recording, e.g., a malicious TV advertisement or a malware that plays a command so that it's picked up by the virtual assistant*
3) *Device gets compromised from the local network to access information, or to snoop on the user*

Question 4

“SmartCar” is a new device that you can plug into your car to keep track of your driving habits and patterns—as well as your car’s location—directly from your smartphone.

All modern automobiles are equipped with an internal wired network that connects together all the electronic control units (e.g., engine controller, dashboard, parking sensors). This network is used to exchange commands and data, including safety-related ones (e.g., data for the ABS, setpoint of the cruise control). This network is based on the standard known as CAN (controller area network): all messages are broadcast to all control units connected to the network, are not encrypted, and their sender is not authenticated. In order to gather information about how the vehicle is driven, “SmartCar” must be physically connected to the car’s internal CAN network, where it actively exchanges messages with the car’s control units in order to gather the required data.

Furthermore, to display real-time data, “SmartCar” is connected via Bluetooth to the vehicle owner’s smartphone, and sends information about the vehicle’s location to a remote server over a cellular network (3G\4G), so that the vehicle’s owner can constantly track its movements—for instance to remotely locate the vehicle in case of theft.
Consider the following scenario: a vehicle owner installs “SmartCar” in their car.

1. What are the three most valuable assets at risk in this scenario?

1. What are the three most valuable assets at risk in this scenario?

1) *Life/Health of the people inside and around the car*
2) *Owner's private driving data*
3) *The device vendor reputation / car manufacturer reputation*
4) *The vehicle itself*
5) *Smartphone*

2. Suggest at least two potential attack surfaces of SmartCar.

2. Suggest at least two potential attack surfaces of SmartCar.

1) *The smartphone application*
2) *The company's backend*
3) *Physical Access to the vehicle*
4) *Bluetooth/cellular network*

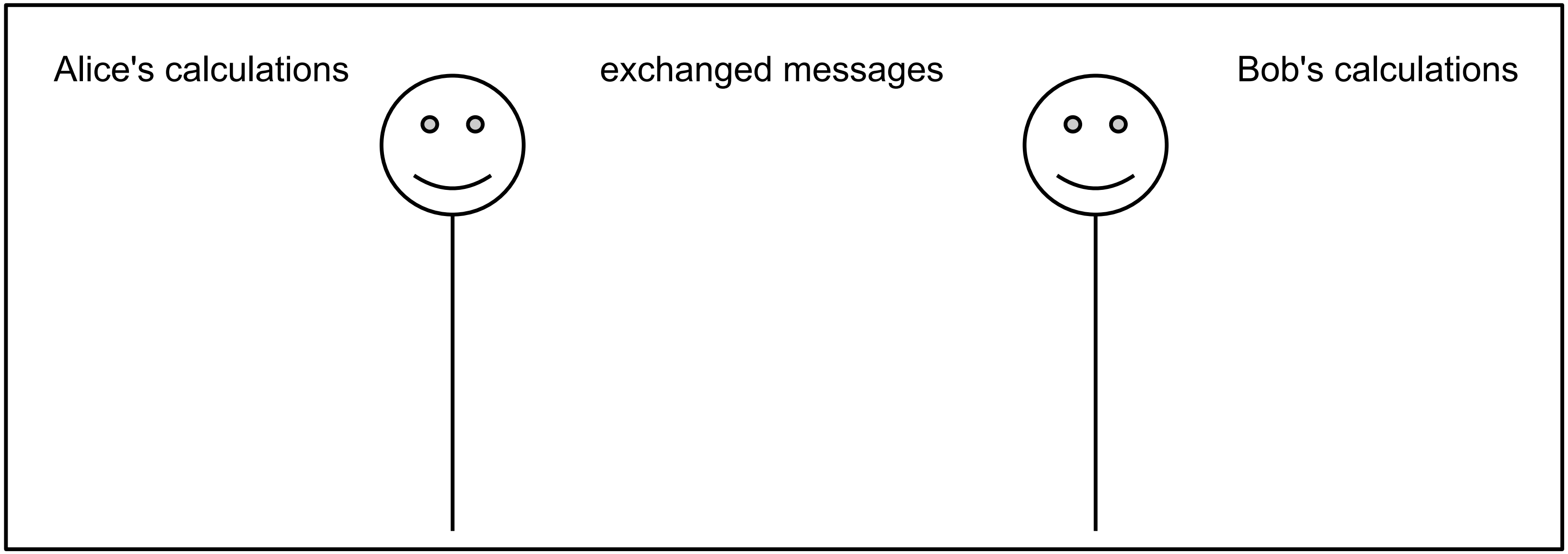
3. Suggest two potential digital attacks in this scenario.

3. Suggest two potential digital attacks in this scenario.

1) *Compromise the company's backend to retrieve all user data… and according to implementation, endanger driver safety by reflashing device and send data inside network*
2) *Physically compromise device to then send commands to the vehicle from remote*
3) *Compromise the application to retrieve data on different users / gather live data on one user*

Question 5

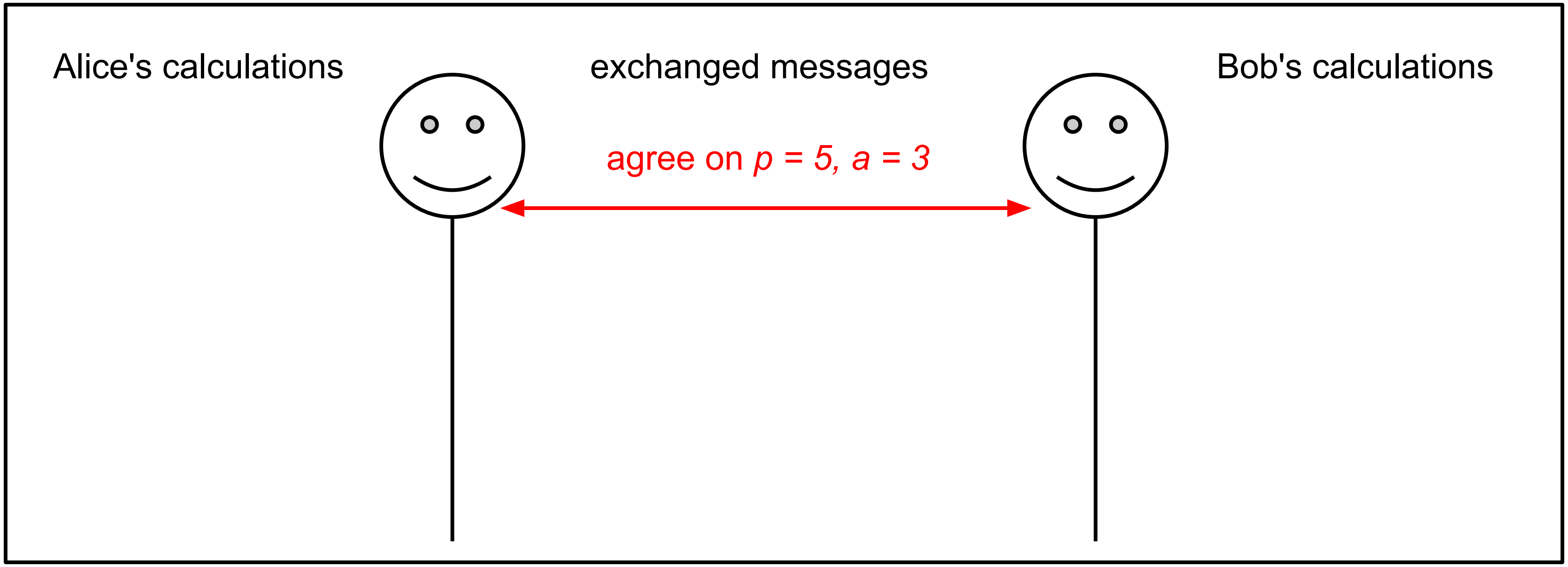
Alice and Bob want to exchange a secret number in a public place and want to make sure that nobody understand. They use a Diffie-Hellman algorithm to exchange a public key. Given the prime p = 5 and its primitive root a = 3, show the exchange and the computation that Alice and Bob need to perform, and the secret that they exchanged.



Alice's calculations

exchanged messages

Bob's calculations

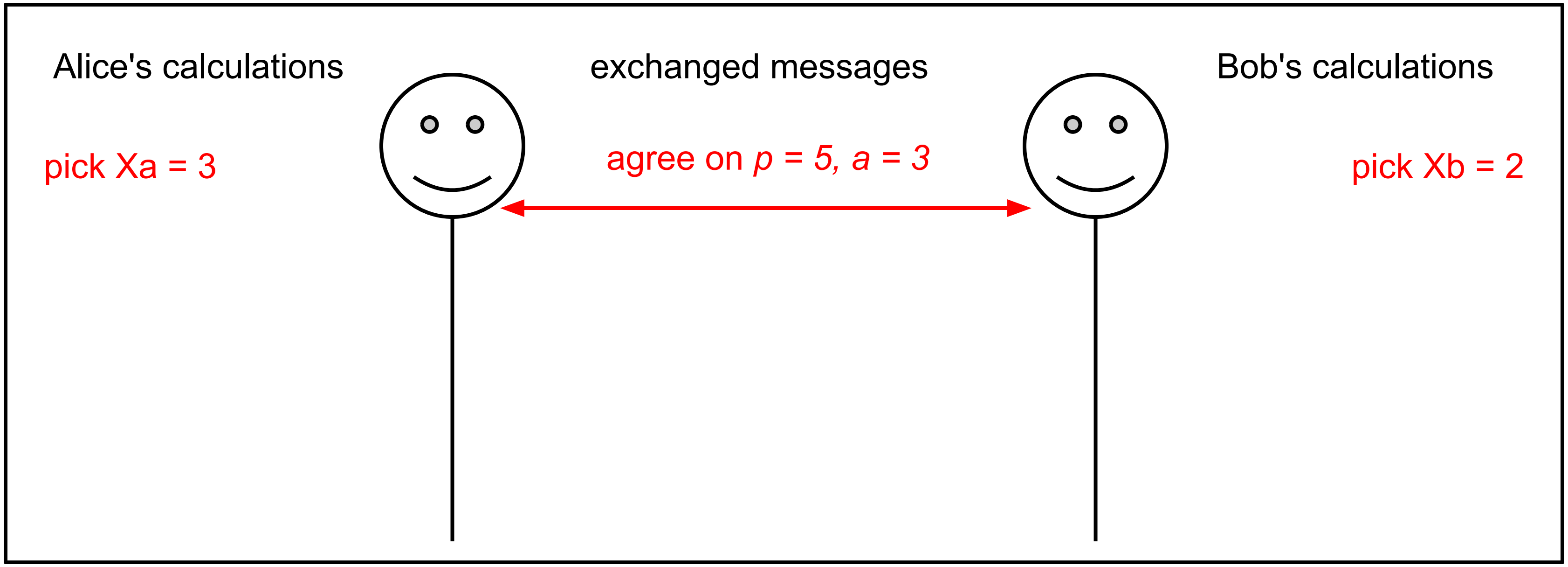


Alice's calculations

exchanged messages

Bob's calculations

agree on *p* = *5, a = 3*



Alice's calculations

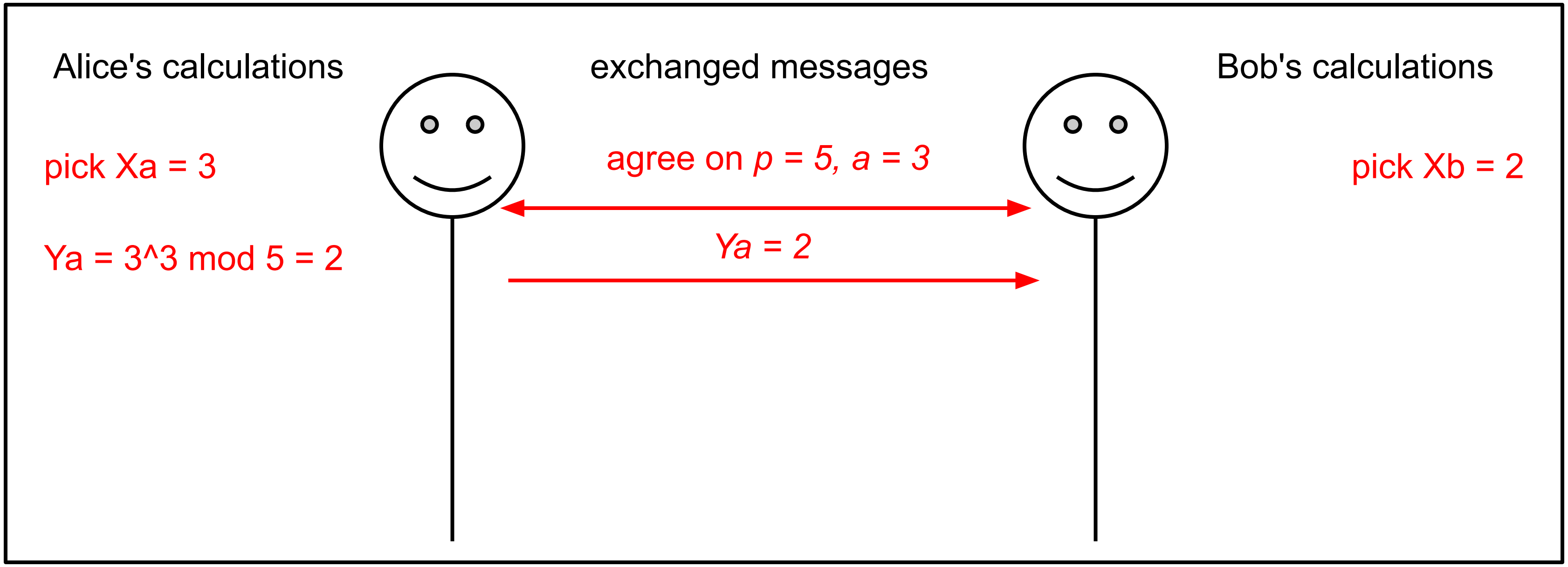
exchanged messages

Bob's calculations

pick Xa = 3

agree on $p = 5$, $a = 3$

pick Xb = 2



Alice's calculations

exchanged messages

Bob's calculations

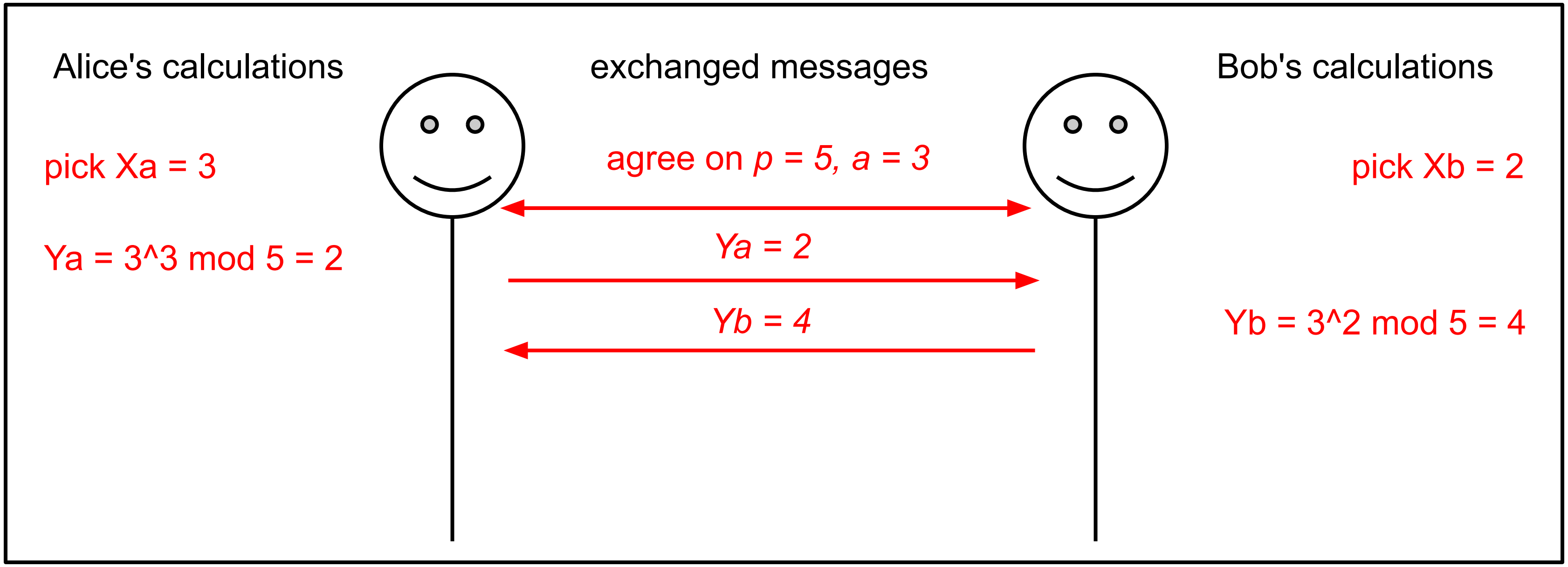
pick Xa = 3

agree on *p = 5, a = 3*

pick Xb = 2

Ya = 3^3 mod 5 = 2

Ya = 2



Alice's calculations

exchanged messages

Bob's calculations

pick Xa = 3

agree on *p = 5, a = 3*

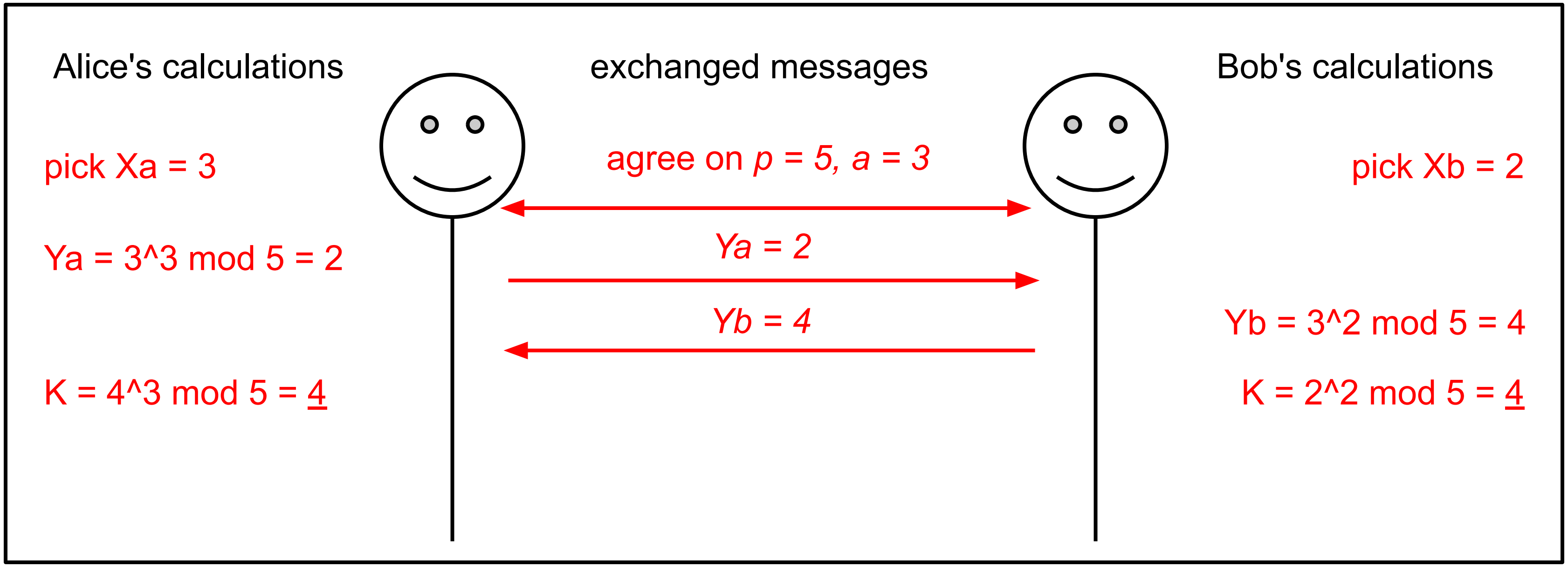
pick Xb = 2

Ya = 3^3 mod 5 = 2

Ya = *2*

Yb = *4*

Yb = 3^2 mod 5 = 4



Alice's calculations

exchanged messages

Bob's calculations

pick Xa = 3

agree on *p = 5, a = 3*

pick Xb = 2

Ya = 3^3 mod 5 = 2

Ya = 2

Yb = 4

Yb = 3^2 mod 5 = 4

K = 4^3 mod 5 = 4

K = 2^2 mod 5 = 4

Question 6

You are having a discussion with a friend about cryptography. Your friend makes a series of statements. Please tell us how you would respond (True or False) and motivate your answer.

A. The reason why the 2048bit RSA is more robust to brute forcing that a 256bit AES, is because the key is longer.

B. No encryption algorithm is perfect, as they are all vulnerable to brute forcing.

C. An encryption algorithm is broken when there is at least one way to derive the key from a given amount of ciphertext.

A. The reason why the 2048-bit RSA is more robust to brute forcing that a 256-bit AES, is because the key is longer.

A. The reason why the 2048-bit RSA is more robust to brute forcing that a 256-bit AES, is because the key is longer.

[see slides on "cryptography"] *False. The size of the key cannot be used as a <u>direct</u> comparison criterion because RSA is asymmetric, whereas AES is symmetric.*

B. No encryption algorithm is perfect, as they are all vulnerable to brute forcing.

A. The reason why the 2048-bit RSA is more robust to brute forcing that a 256-bit AES, is because the key is longer.

[see slides on “cryptography”] *False. The size of the key cannot be used as a direct comparison criterion because RSA is asymmetric, whereas AES is symmetric.*

B. No encryption algorithm is perfect, as they are all vulnerable to brute forcing.

[see slides on “cryptography”] *False. The one-time pad is invulnerable because each ciphertext decrypts to every possible plaintext.*

C. An encryption algorithm is broken when there is at least one way to derive the key from a given amount of ciphertext.

A. The reason why the 2048-bit RSA is more robust to brute forcing that a 256-bit AES, is because the key is longer.

[see slides on "cryptography"] *False. The size of the key cannot be used as a direct comparison criterion because RSA is asymmetric, whereas AES is symmetric.*

B. No encryption algorithm is perfect, as they are all vulnerable to brute forcing.

[see slides on "cryptography"] *False. The one-time pad is invulnerable because each ciphertext decrypts to every possible plaintext.*

C. An encryption algorithm is broken when there is at least one way to derive the key from a given amount of ciphertext.

[see slides on "cryptography"] *False. Generally, a cryptosystem is broken if there is any attack faster than brute force to obtain either the key or the plaintext.*

Practical Crypto Challenges

http://overthewire.org/wargames/krypton/

The End