CS5285
Tutorial 6

Entity authentication

- A verifier only sends/receives messages, i.e. digital data.
- To check that the principal is online the verifier need to establish:
  - that the messages came from the principal (origin authentication),
  - and that the messages have been recently generated (freshness).
- If both conditions are satisfied then we have authenticated the claimant.

Question 1

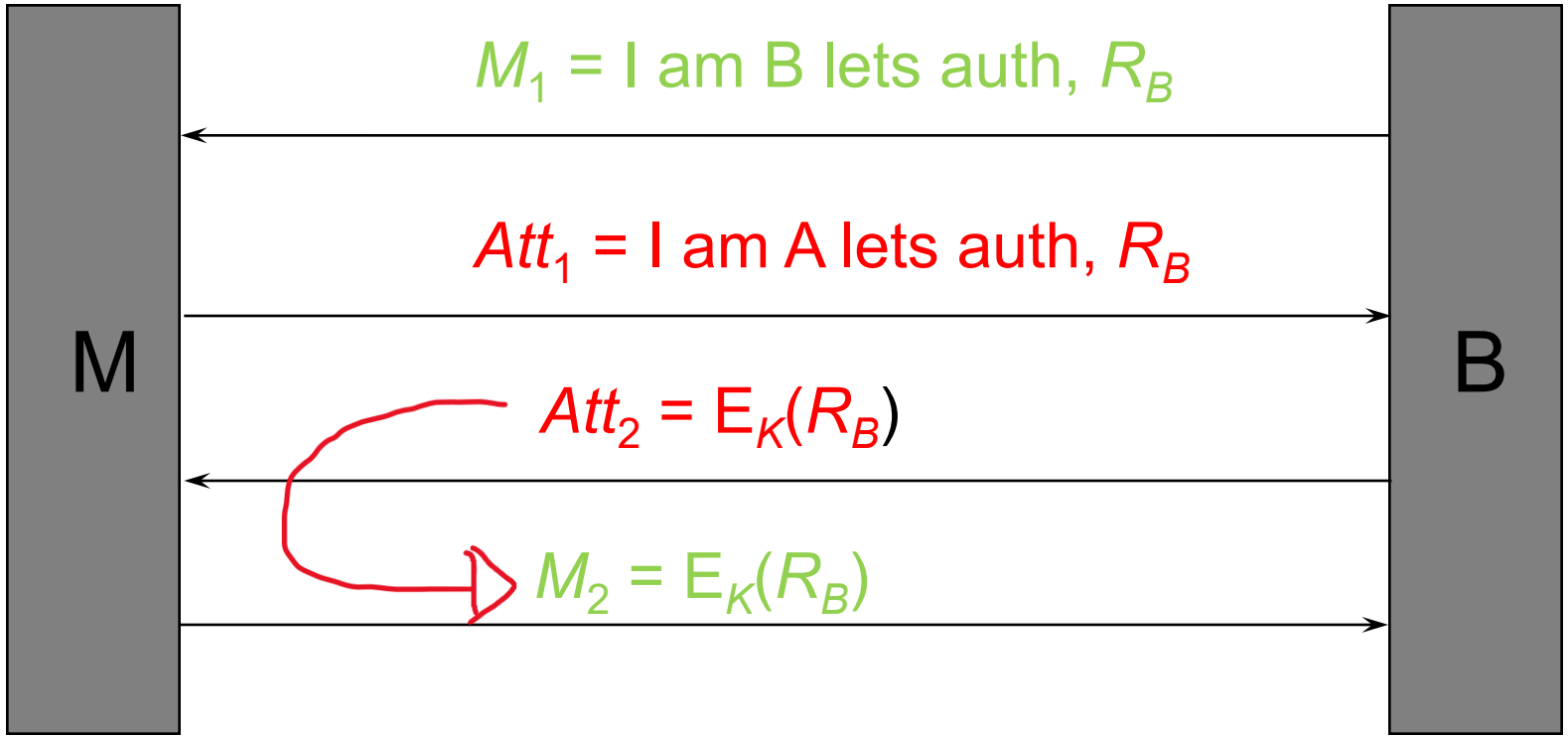
What is the main issue with the following protocol and how would we fix it?

1: A < B: RB

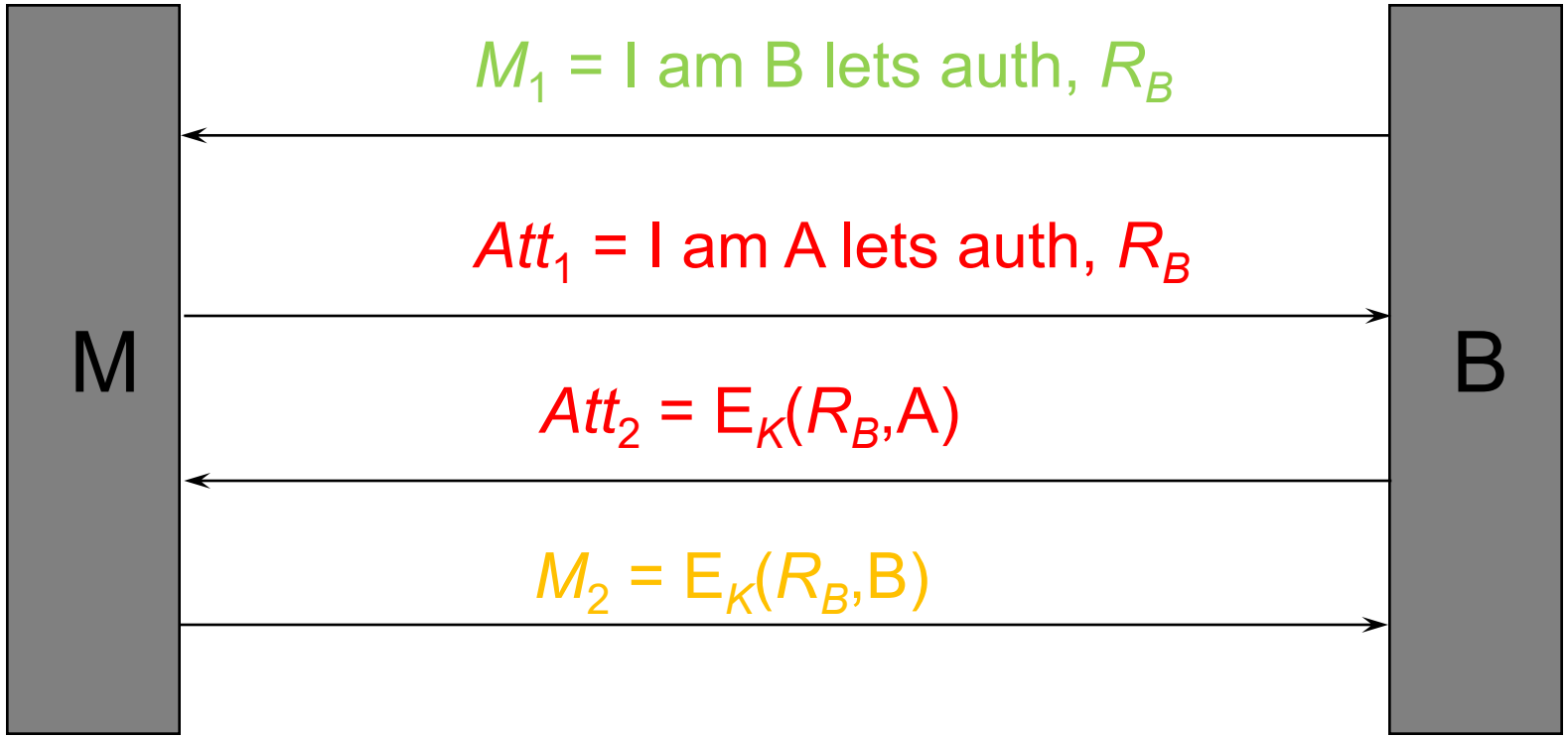
2: A > B: E_K(RB)

Would the issue still be there if message 2 was Sig_A(RB)?

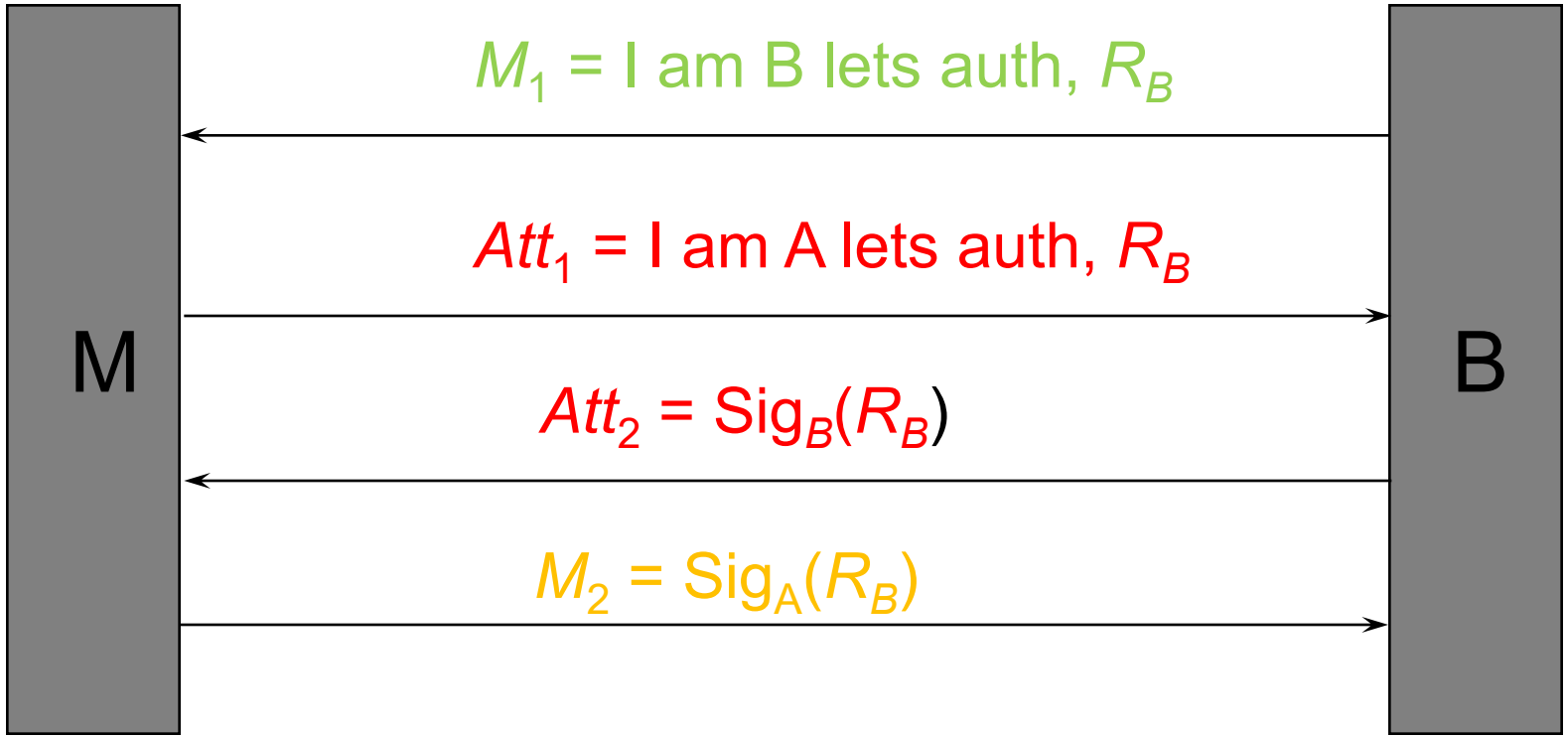
Reflection attack



Add identifier



What if we sign nonce?



Question 2

Could N be any type of nonce in this protocol?

1: A < B: E_K(N,A)

2 : A > B: N

In theory a nonce could be a random number or counter (number only used once)

In this case a counter would be predictable, if an attacker see protocol with N knows next correct response is N+1. So it has to be a random number.

Question 3

Design a unilateral authentication protocols using

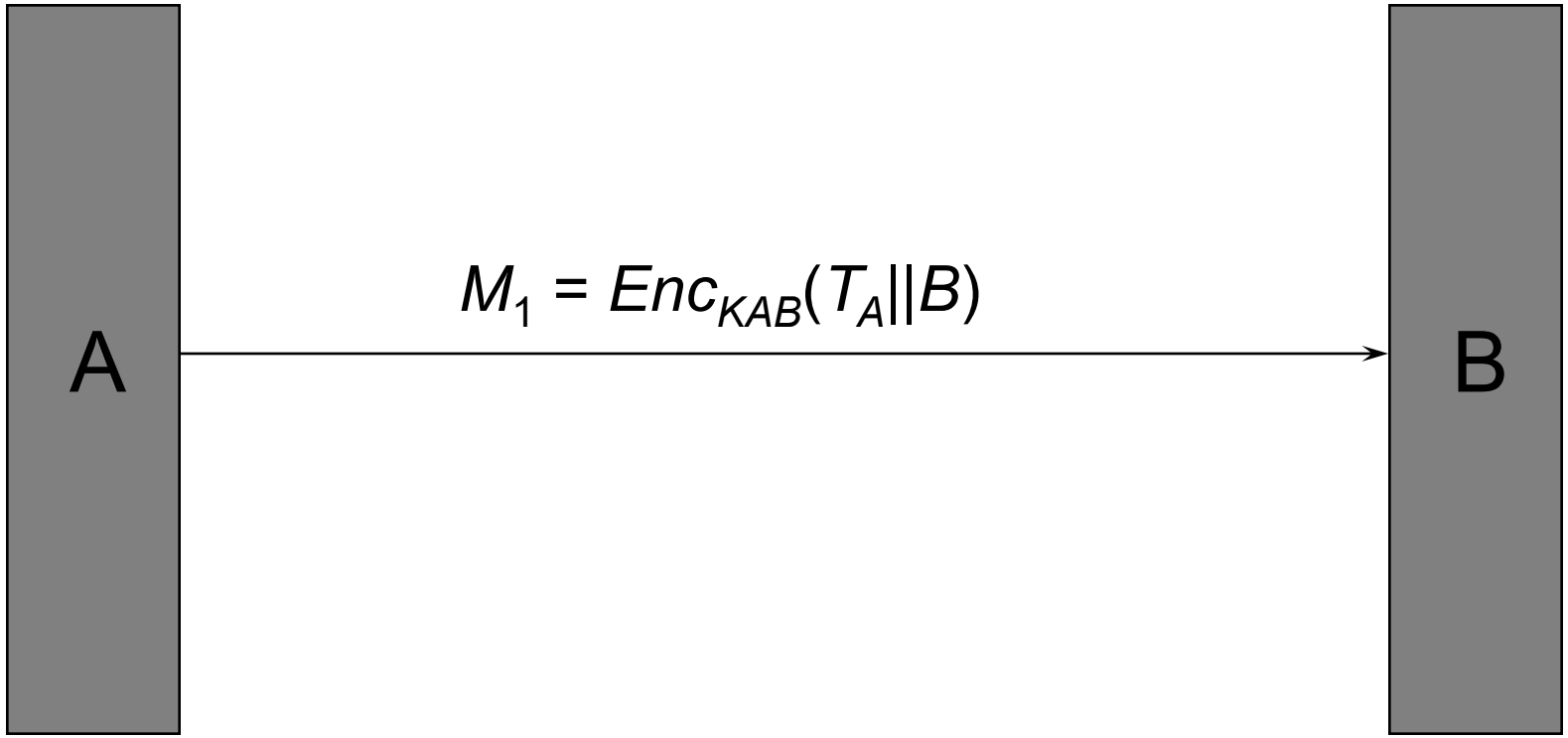
a) A timestamp and an encryption mechanism

b) A timestamp and a MAC mechanism

c) What is the practical difference in how we send the timestamp between a) and b)?

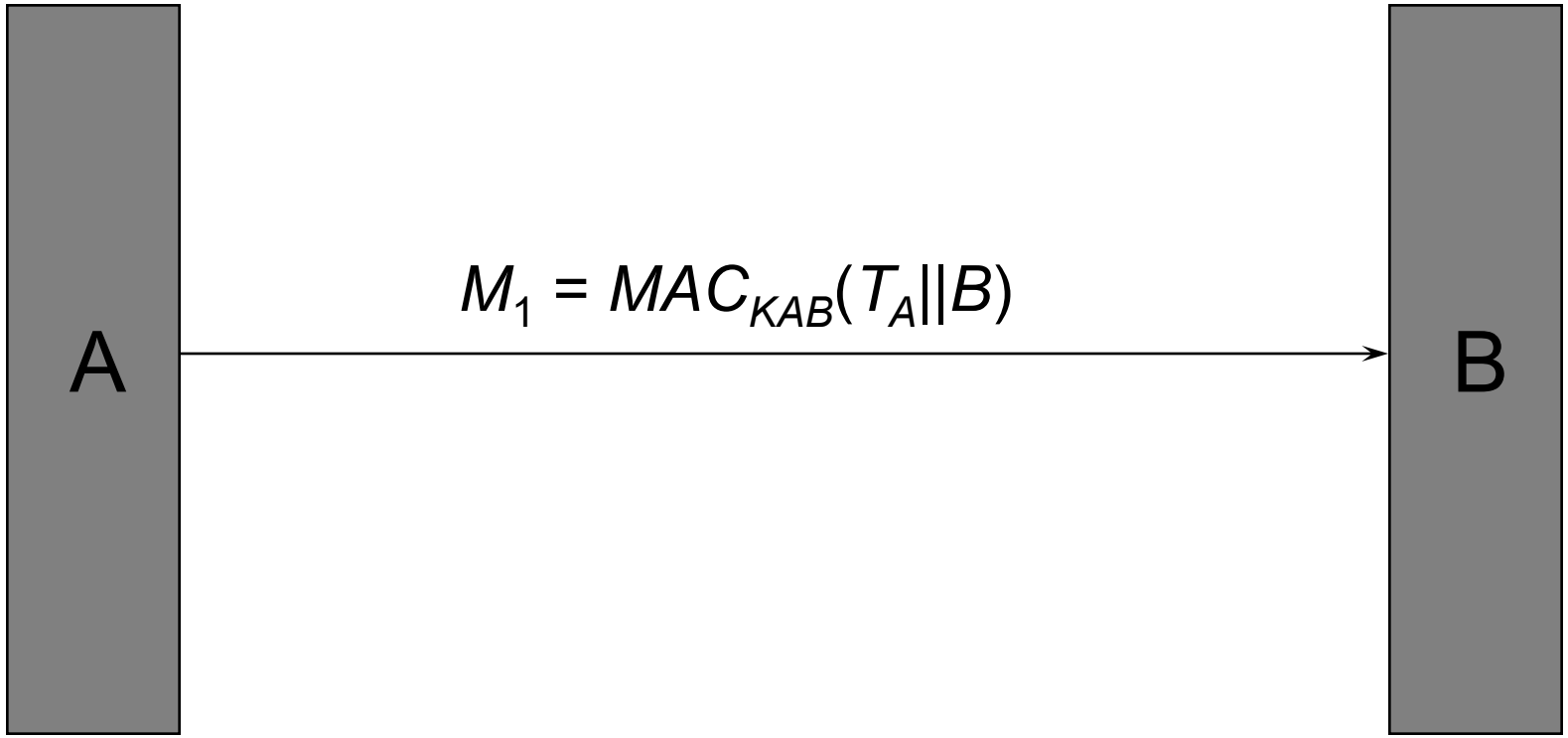
Question 3

Design a unilateral authentication protocols using
a) A timestamp and an encryption mechanism



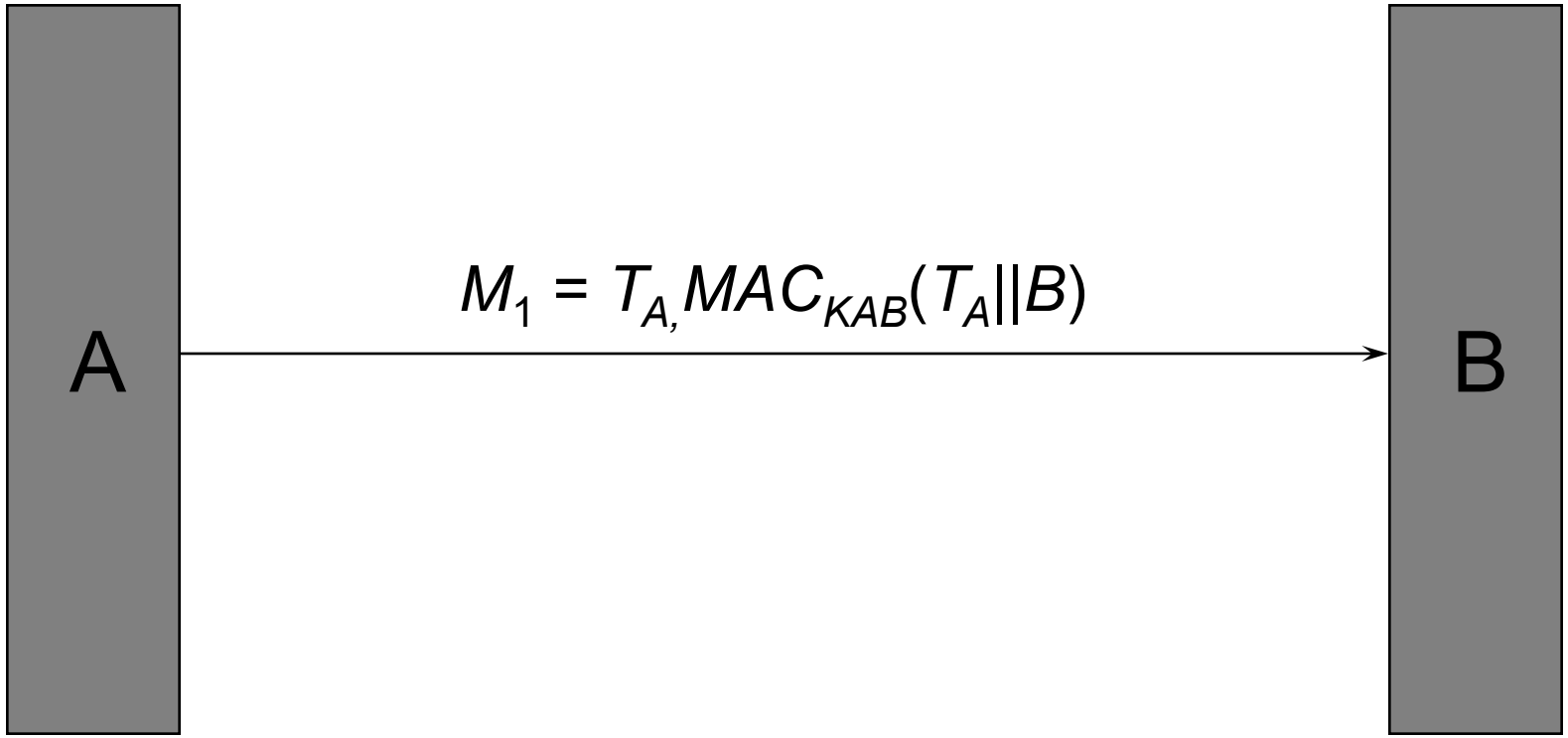
Question 3

Design a unilateral authentication protocols using
b) A timestamp and a MAC mechanism



Question 3

No, does not work…looks secure but not practical
What is the practical difference in how we send timestamp



Question 4

You are asked to design an authentication protocol whereby a web client can authenticate servers he wishes to visit.

You must make the following decisions and design the most practical protocol....

- Time stamp or nonce?
- Symmetric or asymmetric mechanism?

How many clients and servers?

What can we assume about clients?

Question 4

Using nonce or timestamp?

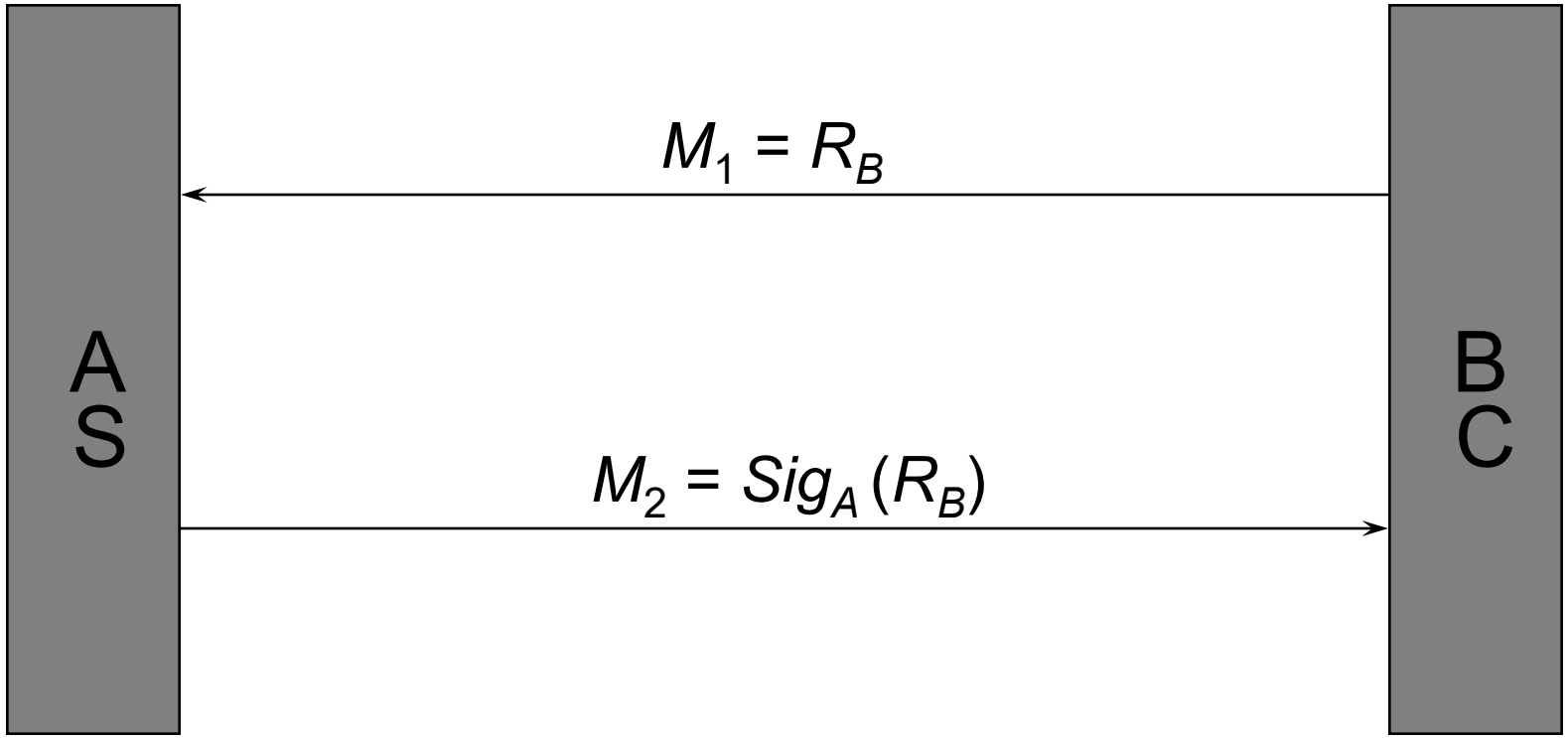
Client not guaranteed to have right time! How does he verify server?

Keys – asymmetric or symmetric?

Symmetric key between all clients and servers?

Use asymmetric mechanism

Question 4



Question 5

You are asked to design an authentication protocol whereby a client can log onto online banking.

You are asked to do so for two banks - both banks gives the client a secure hardware device that can generate a response.

a) Bank 1 device has a single button, and response is generated upon press of button.

b) Bank 2 has a small 10-digit numeric keypad, and also a button to press for response generation?

Question 5a

a) Bank 1 device has a single button, and response is generated upon press of button.

Using nonce or timestamp?
How would you use the nonce? Need to use timestamp.

Keys – asymmetric or symmetric?
Symmetric key between a bank and device?
Use symmetric mechanism

Question 5a

D

$M_1 = Enc_{KDB}(T_D||B)$

B

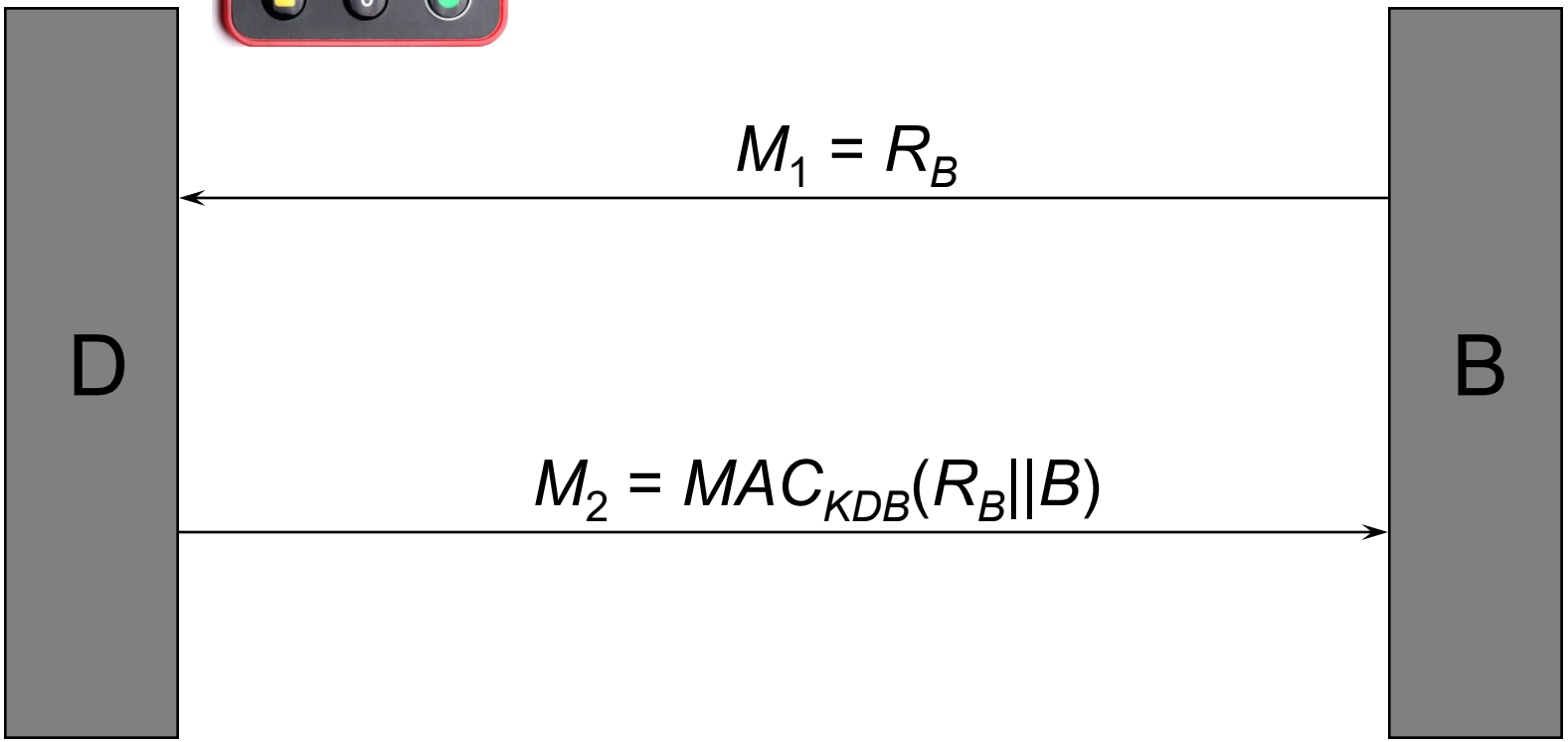
Question 5b

a) Bank 2 has a small 10-digit numeric keypad, and also a button to press for response generation?

Using nonce or timestamp?
Use a nonce, display user a number to type in.

Keys – asymmetric or symmetric?
Symmetric key between a bank and device?
Use symmetric mechanism

Question 5b



The end!

Any questions…