­­­633 – Possible Midterm Questions

# These are the four possible questions regarding the midterm.

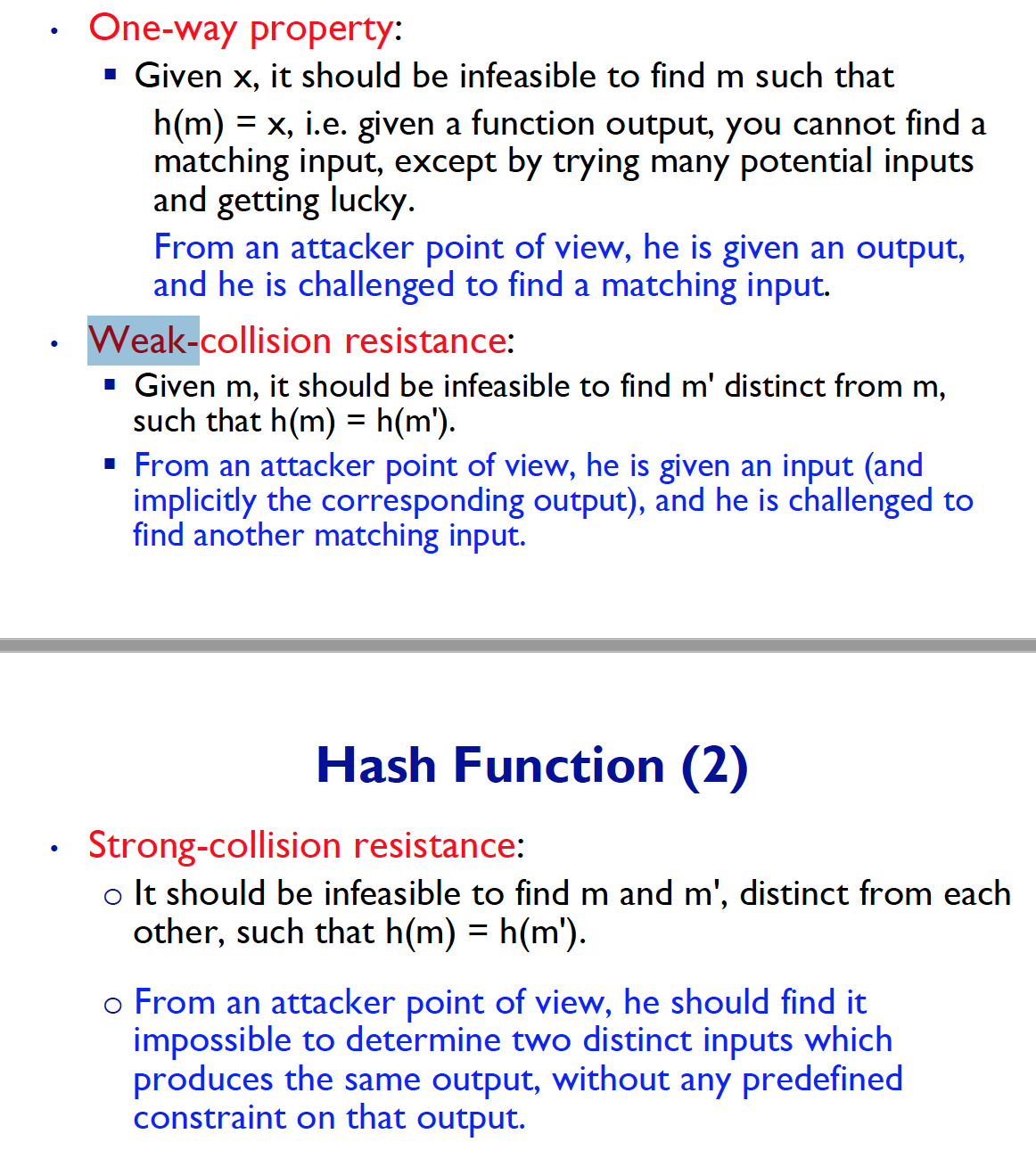
## (a) What is hash function?

## (b) How RSA algorithm

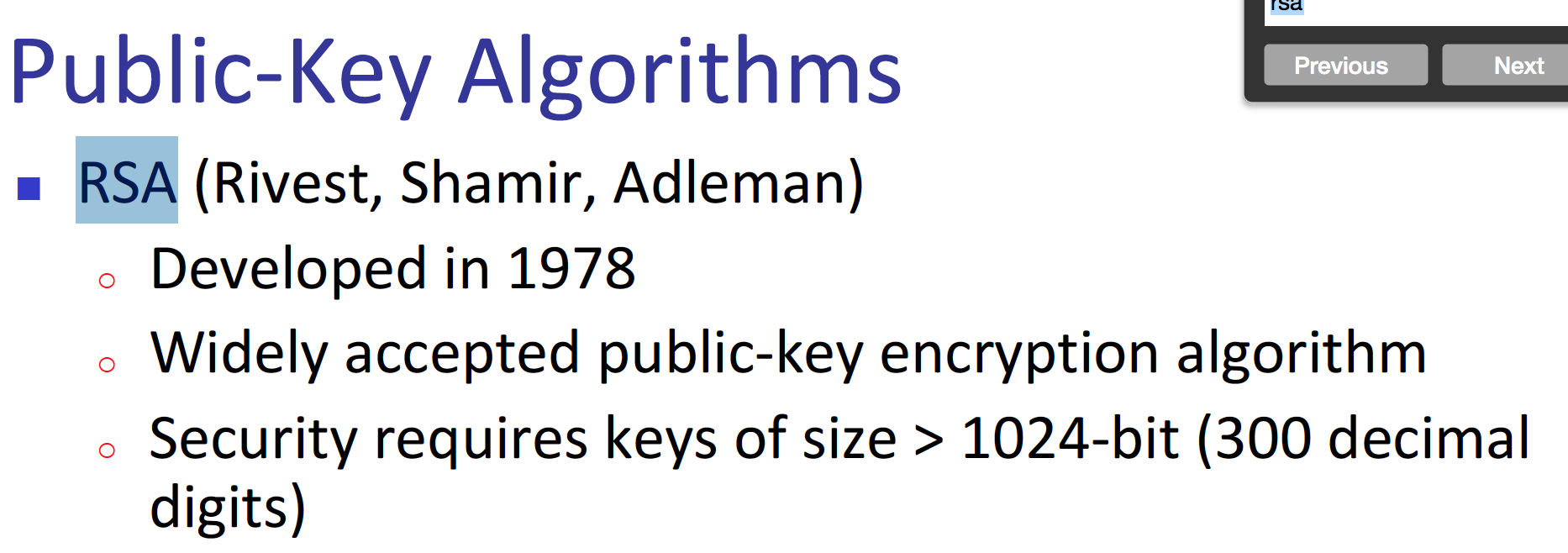
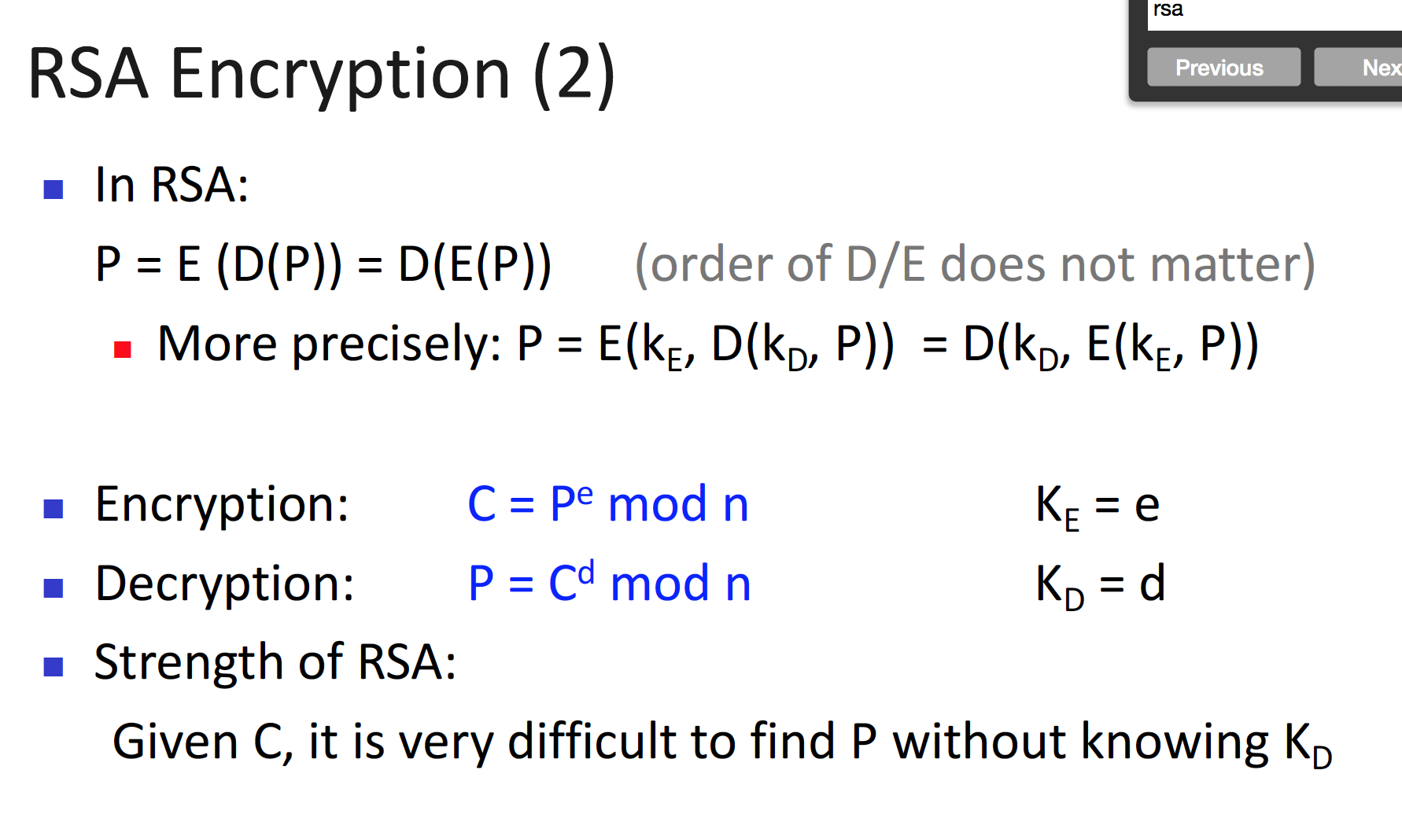
## (c) MD5 algorithm

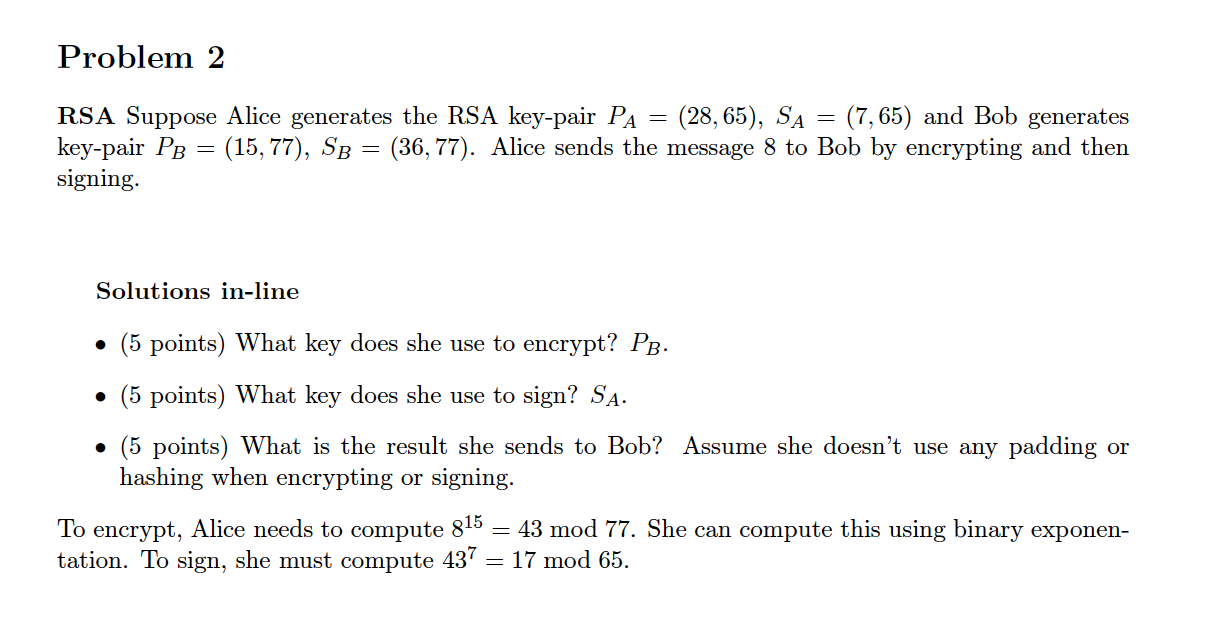
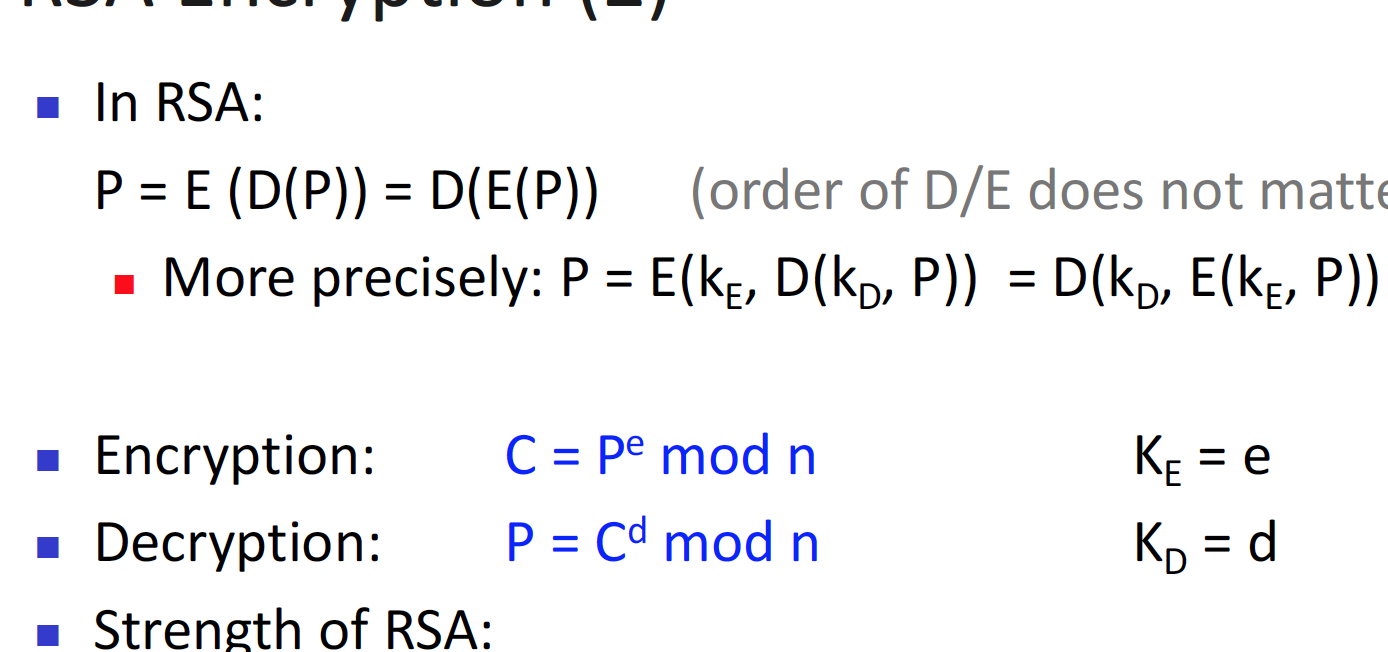
## (d) AES: Electronic Codebook (ECB) vs. Cipher Block Chaining (CBC) modes

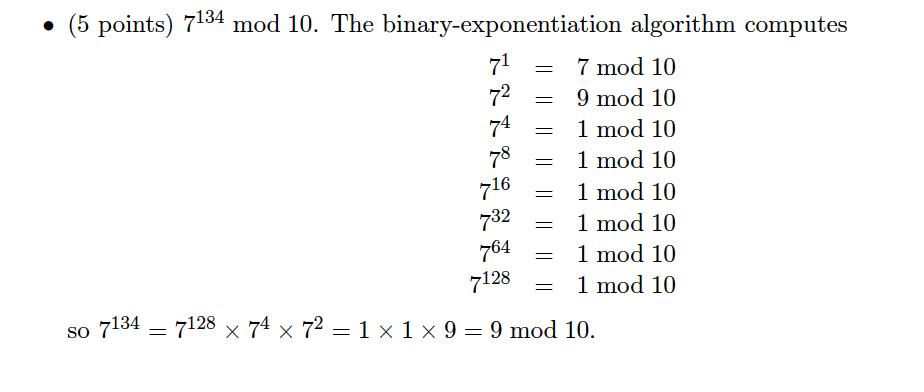
## **What is hash function?**

* Please refer to page 46 of lecture one. In that page it describes the use of the hash function, and what it does to the data. One of the very important aspect of the hash function is the one way property – this means assume that there are three things. 1) h() – the has function, 2) m – plain text message, 3) h(m) = hashed – the encrypted value of the plain text using the hash function. Then it is nearly impossible to get m from the hashed value.   
    
  There are also weak/strong collision property of the hash function. These are best described in this way. Weak collision, h(m) = h(m’) where the m’ is another not the same value as m, but results the same hashed value as m. When hacker knows the value of m then it is very possible for them to obtain the value of m’. – This property must prevent from this happening.  
    
  One other property of the hash function is the strong collision property. Using the same, setting as above, but the difference is when, the attacker does not have the value of m. The attacker have to find both the value of m and m’.   
    
  Finally, just for reference, we learned one example of the hash function. Which is the LMHash function. For more information please refer to page 38 of lecture 2. (NTLM)   
  And LMHash is very weak hash function, (no salt and only printable ANSCI)   
    
  

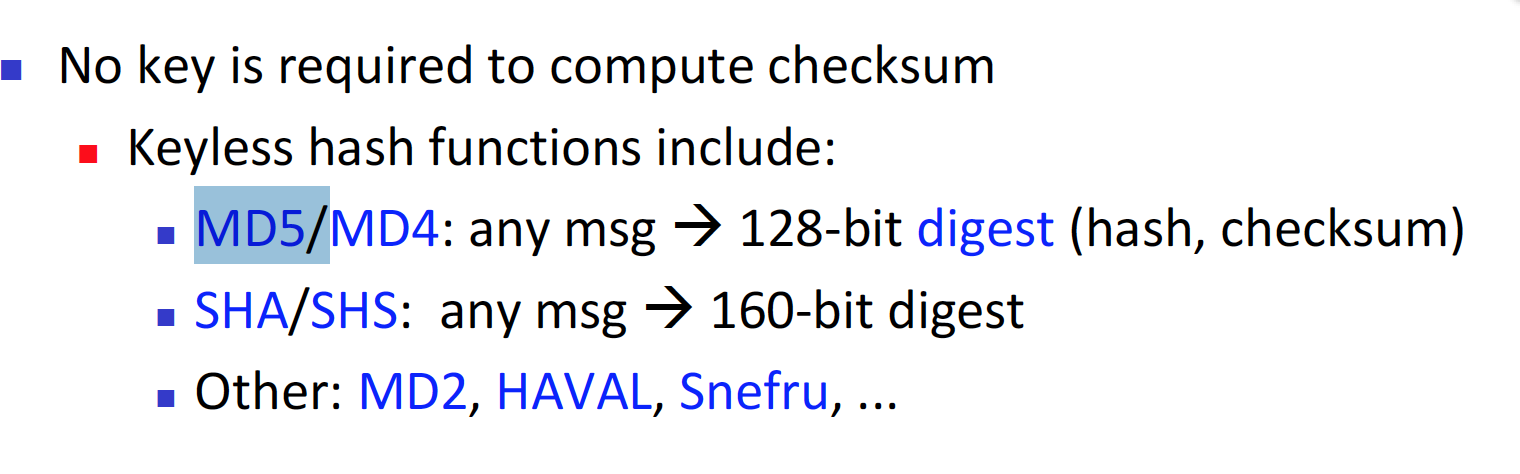
## **How RSA algorithm**

* RSA algorithm is relatively slow algorithm, and to know more about this algo, please have a look at page   
  Full name of RSA: Rivest-Shamir-Adelman   
  ^ from there we can already know that, this is an asymmetric algorithm. Symmetric key algo does not need a public key, rather the secret key is exactly the same as when encryption happens and decryption happens.  
  Please look at page 19 of lecture – 4, this describes exactly how the RSA algo works.  
  Also, below is some problem that can help understanding the data little bit more better. 

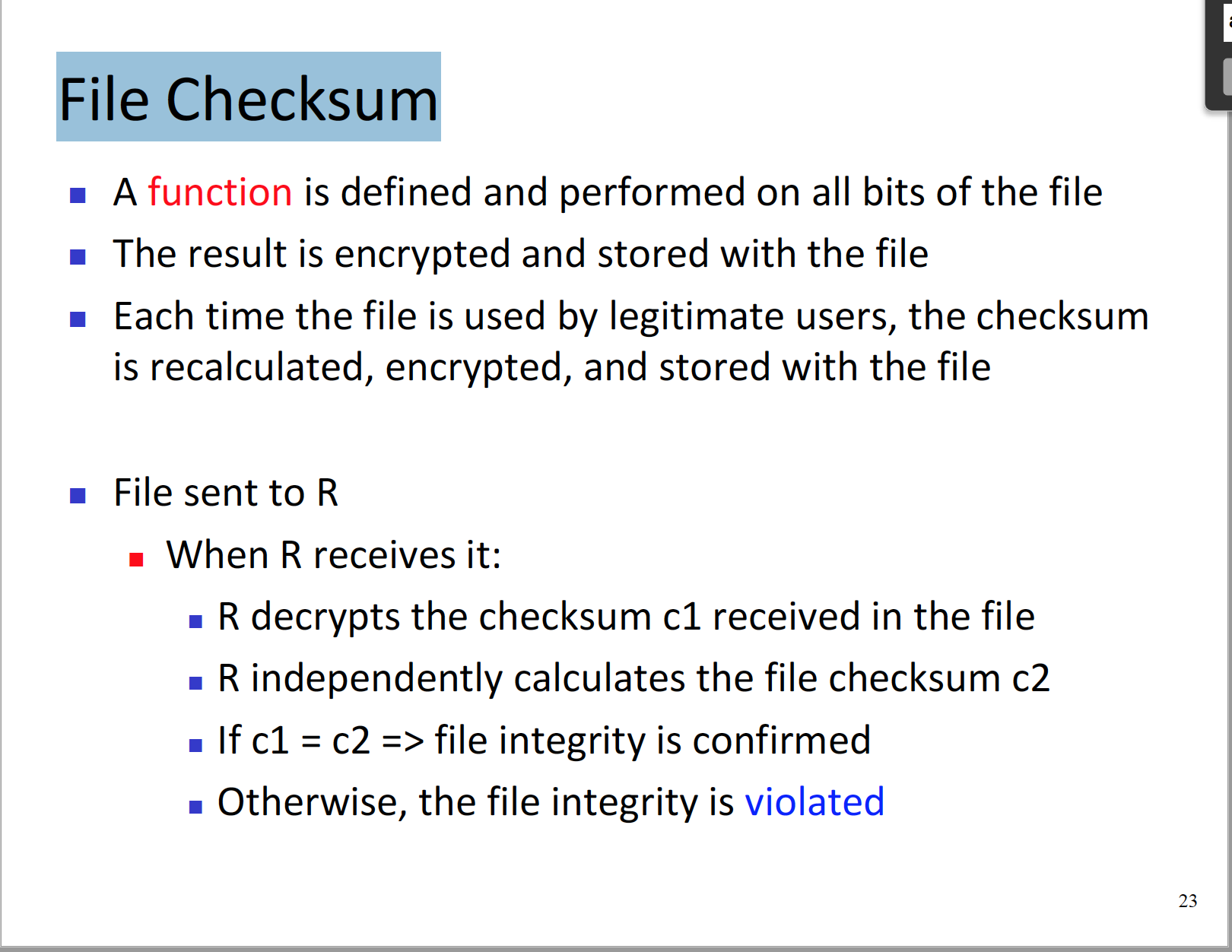
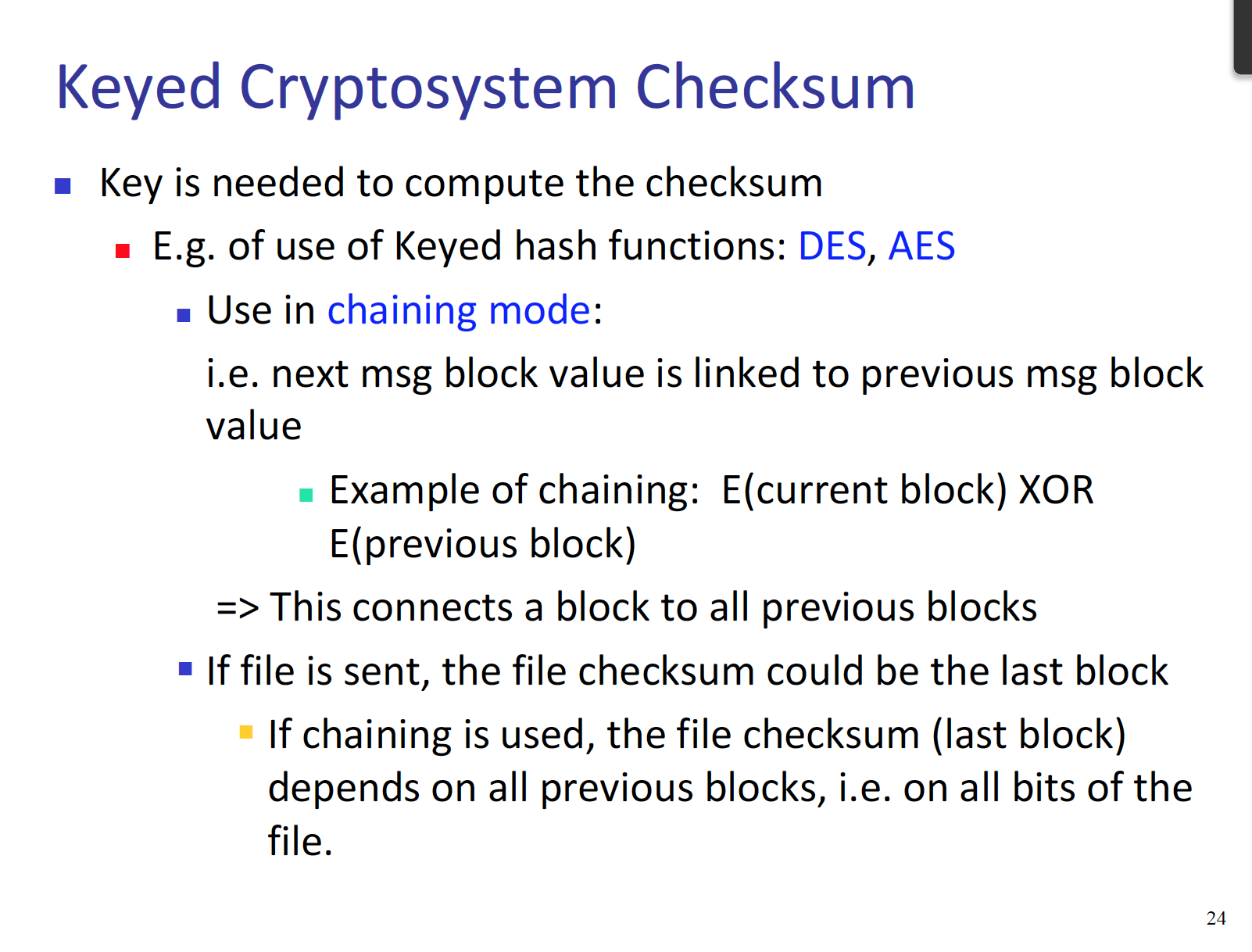
tackling the RSA ke = private key, then the kd = public key of A.  
so the mathematical function is module!   
The above mathematical explains the steps of module.



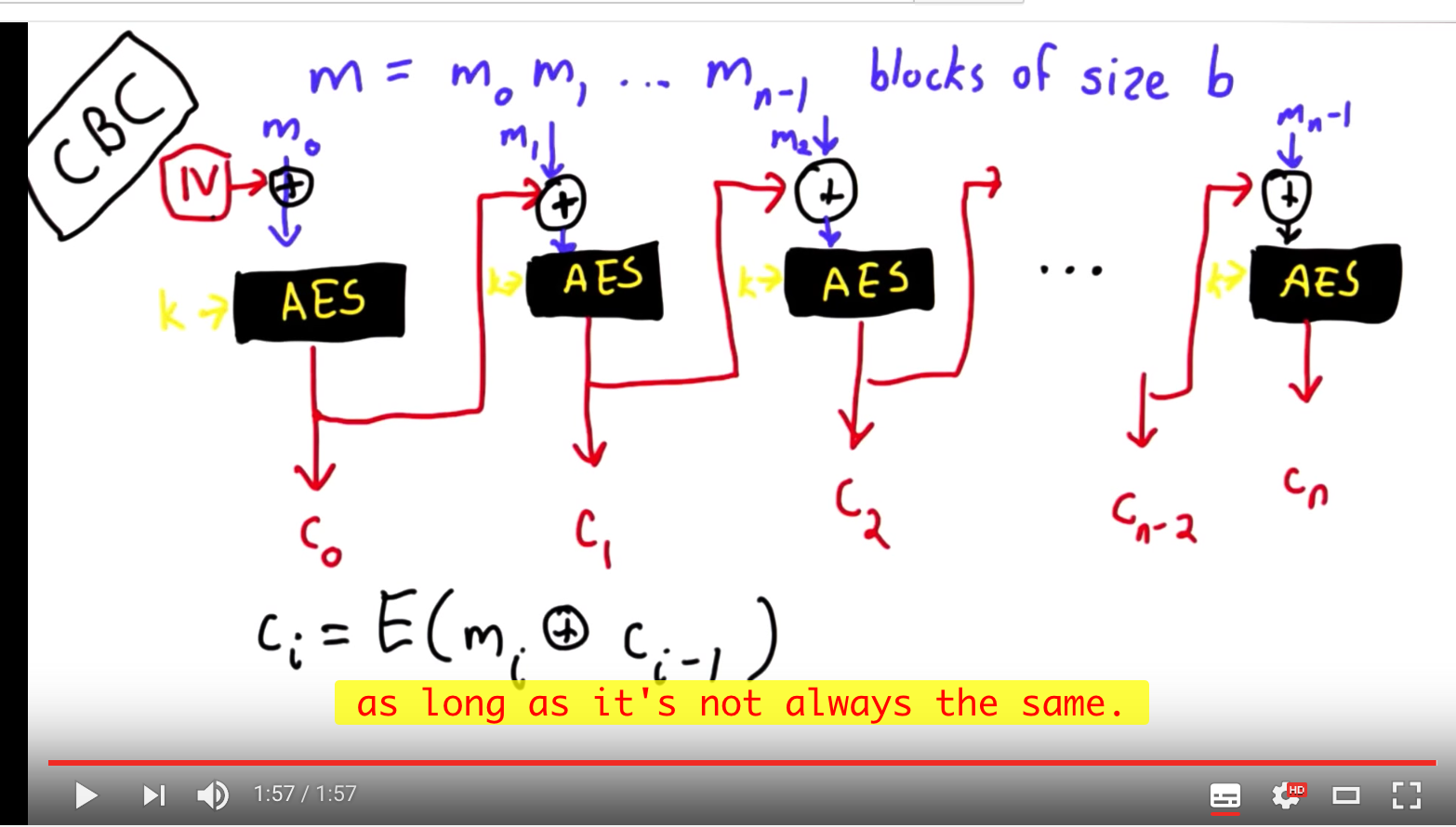
## **MD5 algorithm**

* We learned that MD 5 is a keyless Cryptosystem Checksum, this means that the algo does not need the key, in order to check if there are some bits that have been, altered.
* Also, one note – checksum only checks the integrity of the data, does not perform message authentication.  
    
  ^ THE PROBLEM IS THIS IS THE ONLY, FUCKING DESCRIPTION REGARDING MD5 LOL – SO WE NEED GOOGLE TO HELP US!
* This video shows the power of MD5 alog : <https://www.youtube.com/watch?v=33QT7xohUvI>
* MD5 is a checksum algo algorithm, that check the integrity of the data, file size maybe still the same, however the MD5 check sum is different if the file has been changed.  
  <https://www.youtube.com/watch?v=X0TtgwQT0lE> <- for a tutorial on MD5
* <http://md5encryption.com/> <- you can try it on your self.
* <http://www.fastsum.com/rfc1321.php#Description> <- explanation on how the MD5 actually work.
* ***OCT 31 – ASK THE PROF OF STEP BY STEP EXPLANTION OF THE MD5 HASH FUNCITON.***

## **AES: Electronic Codebook (ECB) vs. Cipher Block Chaining (CBC) modes**

* Before we look at what AES is and also what ECB is, we need to know the meaning of file checksum. Remember in computer networking, this term was used. When sending one packet to from one host to another, there can be 4 source of delay. 1) Queue, 2) Processing, 3) Propagation and 4) Transmission delay – however, with these delays there can be bit error, or any kind of change in the bit. So! We need a way to tell the client that the server has send a packet, that is no changed – Chapter 3 of computer networking deals with this matter to very detailed, extent.   
    
  ANYWAY! We learn this concept in computer security too, but the perspective of security rather than network.
* And within the file check sum mechanism, there is a keyless, and key needed algo.   
  and AES is one of the key needed algo that performs check sum.   
  ^LOL THAT IS IT FOR THE EXPLANTION OF AES, THE SLIDES DOES NOT EVEN HAVE ANYTHING ON CIPHER BLOCK CHAINGING – SO LETS GO TO GOOOGLE!!!  
  AES – Advance Encryption Standard  
    
  And AES was born because DES cipher was able to be broken.

## **Cipher Block Chaining (CBC) modes**

* This video from Udacity : <https://www.youtube.com/watch?v=0D7OwYp6ZEc>  
  
* Cipher Block Changing is basically described as above. The original message is encrypted using the AES function. Then the newly encrypted data which is c0 is used as a key to encrypt another set of data, - from original message – this pattern continues on for a while. And remember that in the beginning of the process the original message is divided into chucks of data. BLOCK SIZE OF B
* AES – this means (Advanced Encryption Standard)  
  ^ To know how this process is being done, please read the “lec3\_complements\_AES.pdf” which is included in the lecture 3 pdf – in this pdf, all of the things are very well explaned.

Recap of all of the algo we need to know!

1) RSA – Public Key encryption algo – this is encrypting and decrypting the data

2) MD5 – keyless checksum algo, so this is a hash algo. Meaning there is no reason for to recover the cipher text for the plain text. Just to check the data integrity.

3) AES/DES – Keyed symmetric encryption algo – need to perform deception in order to retrieve the plain texts

4) CBC – AES based keyed checksum algo. This is techn, in which the previous next block of message depends on the previous block. Since it uses AES as the hash algo, so it needs a key to perform hash function.