Arab Academy for Science Technology and Maritime Transport
College of Computing and Information Technology

Course	Computer System Security
Course Code	CS421
Lecturer	Prof. Dr Ayman Adel
TA	Maram Shouman, Menna Elmasry

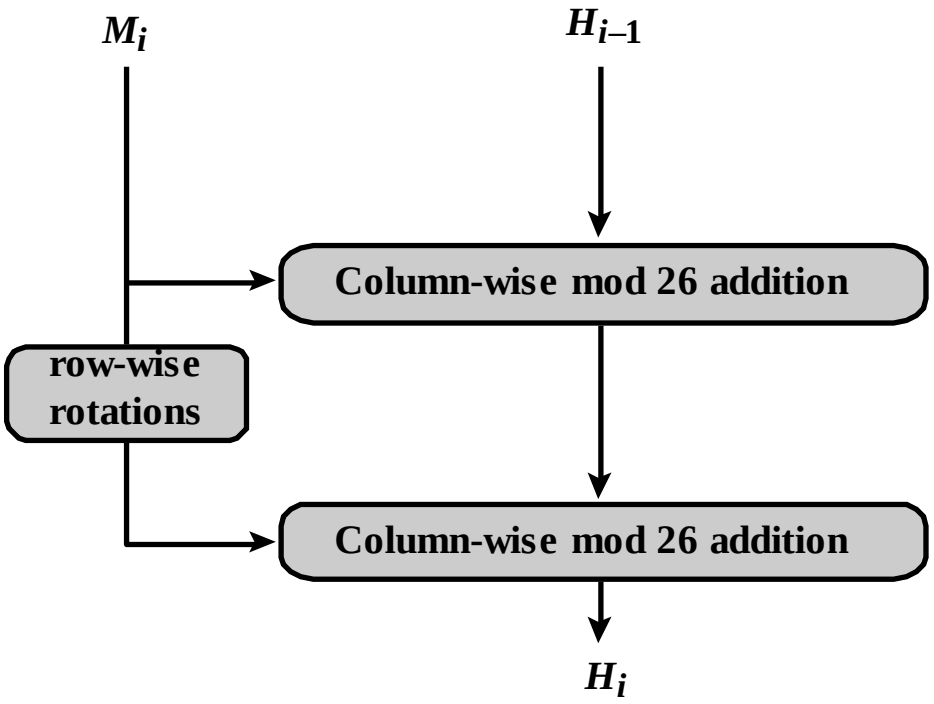
Sheet 8

Review Questions: (2 marks per each question)

1. What characteristics are needed in a secure hash function?
2. What is the difference between weak and strong collision resistance?
3. What is the role of a compression function in a hash function?
4. What types of attacks are addressed by message authentication?
5. What two levels of functionality comprise a message authentication or digital signature mechanism?
6. What are some approaches to producing message authentication?
7. When a combination of symmetric encryption and an error control code is used for message authentication, in what order must the two functions be performed?
8. What is a message authentication code?
9. What is the difference between a message authentication code and a one-way hash function?
10. In what ways can a hash value be secured so as to provide message authentication?
11. Is it necessary to recover the secret key in order to attack a MAC algorithm?

Problems: (5 marks per each question)

1. Consider the following Hash function that operates on letters instead of binary data. Each block of 16 letters is arranged as row wise 4*4 block of text and is converted into numbers (A=0, B=1, C=2, ...). The output of each round is the sum of each column and the initial vector mod 26. The row wise operation is done by circular rotation of each row to the right according to the order of the rows. Show the output of the hash function considering the following message ABCDEFGHIJKLMNOP with IV = 0000.



2. It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible?

3. Suppose H (m) is a collision-resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages x, x′ with $x \neq x'$, we have $H(x) \neq H(x')$ Explain your answer