**MIS 6330: IT Security**

**Individual Homework 2**

**(Write in your own words. Do not copy/paste from online resources or the text. This is an individual assignment, so if I receive identical answers, I will treat them as instances of academic dishonesty.)**

1. One secret key is required for two people to communicate via a *symmetric* cipher.

In the case of *stream* cipher, this key (**K**) is used as seed for pseudo-random number generator to generate (**ki**) bit used to XOR with byte stream of message.

1. **M**essage **A**uthentication **C**ode (**MAC**) is basically a code appended to the original message.

It is calculated by performing operations on original message and these operations are only known to sender and receiver.

It is primarily used to verify that code received by the receiver.

On receiving the message, the receiver will calculate MAC from the original message again and compare it with the value received along with the message.  
If these values match, the message is authentic and unaltered.

Yes, Digital Signatures can be used as Message Authentication Code.

1. Strong collision-resistance property of a *secure hash function* is critical to implementing *digital signature* as:

The whole concept of digital signature is that we use the digital signature to authenticate that the person who signed the document is the person intended.

If, we find any two digital signatures to match, it should only mean that they are the same person.

For the above condition to be satisfied, strong collision-resistance is very critical.

However, while fulfilling that condition, it will also fulfil weak collision-resistance too.

1. To exchange a secret key, we use Diffie-Hellman key exchange algorithm which uses public-key cryptosystem.

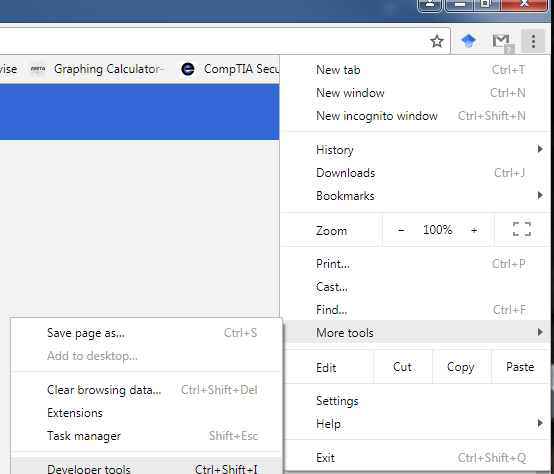
It basically requires two prime numbers (x and y).

Even if the communication is done in untrusted or insecure channel, the users will be able to exchange the key (K).

This key (K) is then used for other algorithms to encrypt the communication.

In each session, we create a new key and never store it.

1. Check Amazon’s *public-key certificate*. List some of the details you can find out about it, e.g., *certification authority* (CA) and Amazon’s *public key*. In Chrome, you can use Developer tools and then select the Security tab to view your certificate.



|  |  |
| --- | --- |
| **Detail** | **Value** |
| Certificate Authority | Symantec |
| Algorithm used for Signature | Secure Hash Algorithm 256 bits with RSA |
| Validity | 30th October 2016 to 31st December 2017 |
| Subject Common Name | [www.amazon.com](http://www.amazon.com) |
| Subject Organization name | Amazon.com Inc. |
| Subject Locality | Seattle |
| Subject State | Washington |
| Subject Country | US |
| Issuer Common Name | Symantec Class 3 Secure Server CA - G4 |
| Issuer Organizational Unit | Symantec Trust Network |
| Issuer Organization name | Symantec Corporation |
| Issuer Country | US |
| Serial Number | ‎1d 4a bd aa 78 d0 9a fe 79 9d 41 bc eb 7a 76 62 |

|  |  |
| --- | --- |
| Public Key | 30 82 01 0a 02 82 01 01 00 c2 5a 28 67 75 9f f8 1f 1c d6 74 d9 8f fd 78 c0 23 c8 8f 28 5c 39 5e 72 b4 46 50 0d bb 5f b5 68 b1 3b 14 e9 1b 64 a5 93 61 88 d6 9c ed 11 2a 68 a4 19 9b 63 f8 5a 33 96 0d 58 36 03 1e bd 35 01 0b f3 02 ac 2c 37 2c f9 b1 7e 2b ca d9 08 11 62 3d d8 3a 26 29 bb f1 40 aa f2 d2 6d 19 ba 3f 4c cd a6 d9 6f 6b c7 6f 47 5b 5b 05 25 db 25 e7 e6 79 5f 1c 94 9f 98 3d 13 4b 75 05 35 a4 33 5c 4c 45 9e 52 94 fe 2e d5 a2 62 c4 07 f3 bd 3a d7 c9 d1 5d 97 67 36 f3 3b 1d d1 7e f4 f2 e7 09 a7 e0 0c 42 0b b9 c6 46 49 4d 04 a5 5a fa 7a 51 97 4c e3 fa 5a 32 09 a3 3e 00 5e 58 57 d6 5b 51 12 2e c5 88 99 39 6d ee d9 ae ba 57 36 30 09 16 b6 11 db 48 6c f0 0b 3b f7 52 ac 53 40 b9 a0 21 2a aa 45 37 43 81 e3 67 75 e8 85 94 38 a8 8c 88 70 c9 2f 9d 76 60 02 49 06 67 d0 3c 8e df 55 0b 57 27 02 03 01 00 01 |
| Public Key Parameters | 05 00 (or NULL) |
| Alternative DNS names | amazon.com  amzn.com  uedata.amazon.com  us.amazon.com  www.amazon.com  www.amzn.com  corporate.amazon.com  buybox.amazon.com  iphone.amazon.com  yp.amazon.com  home.amazon.com  origin-www.amazon.com |