Wasfi Momen

1. Since these urls still leading to valid link locations, therr can be a delay in the click to reveal the true location of thr url and ask if the user wishes to go there. Unpacking the url helps as well.
2. For every item purcashed , a message should be sent from client to server containing the encrypted message amount via the key and a digital signature using a one-way hash function. The server should ACK this message with its own message and digital signature so that nonrepudiation can occur between the two parties.
3. With a key of 3 right shift, INFORMATION SECURITY becomes lqirupdwlrqvhfxulwb.

m=23, a=7

gcd (23,7) = 1

|  |  |  |  |
| --- | --- | --- | --- |
| 23 mod 7 | 3 \* 7 + 2 | 23 - 7(3) =2 | 7 - 2(3) =1 |
| 7 mod 2 | 3 \* 2 + 1 | 7 - 2(3) = 1 | 7 - (23 + 7(3)) (3) = 1 |
| 2 mod 1 | 2 \* 1 + 0 | 2 - 1(2)=0 | 7(4) - 23(3) =1 |

s=-3, t=4 **Multiplicate inverse is 4**



512 = 240(2)+32

240 = 32(7)+16

32 = 16(2)+0

**Gcd is 16**



n=pq

N=(17)(11)= 187

O(theta)=(p-1)(q-1)=160

e = 641

d=e^-1=1 mod O(theta) =

2. Without the ability to manipulate (mutability) the data in the signature and since digital signatures are made using the private key of the user using one-way hash functions they cannot be forged. As such, either user sending a digital signature cannot deny the other's signature in two-way communication.
4. Alice chooses a random key and encrypts the message with her key using a crypto algorithm such that C = Ek(M) where C is the ciphertext, Ek is the encryption algorithm and M is the message

She then encrypts her k by using Bob's public key so only Bob can read it. She then signs her cipertext C with her private key.

She then will send the original ciphertext containing the message, the new ciphertext containing her private key, and her signature.

b) First Bob should verify Alice's signature to make sure the message came from her.

Bob will then proceed to decrypt the cipher text containing Alice's private key by using his own private key to decrypt the message.

After that, Bob will use the key to decrypt the final ciphertext containing Alice's message.

10. Every bitcoin block transaction is broadcasted to the global chain of blocks that every user of Bitcoin must update before the beginning of the next mining block. Going back on blocks is not possible.