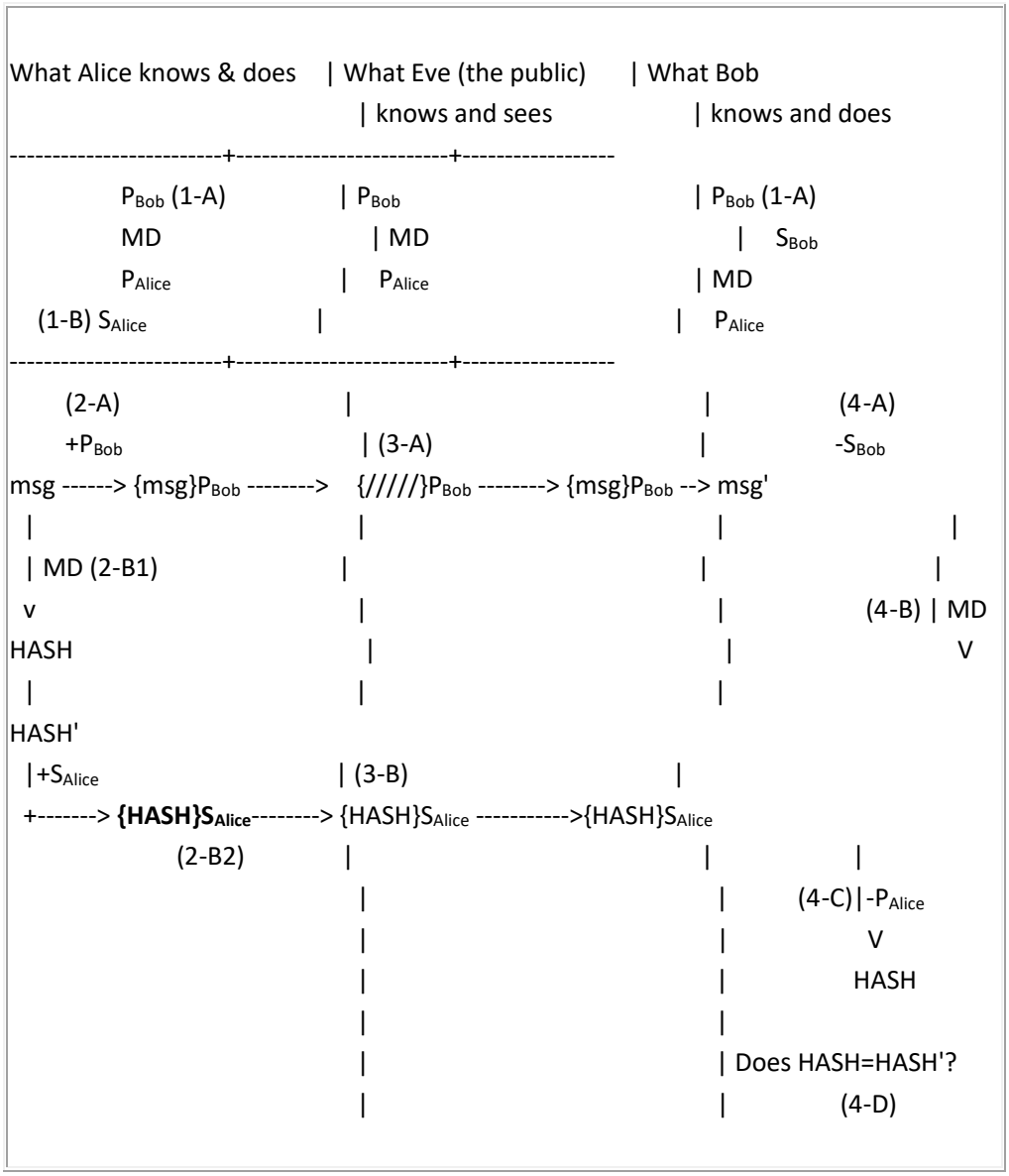
Question:

ECC Crypto Tool .

- Please use ECC Encryption/Decryption Tools and Message Digest Calculator to prove Whitfield Diffie's rules showing in this diagram:



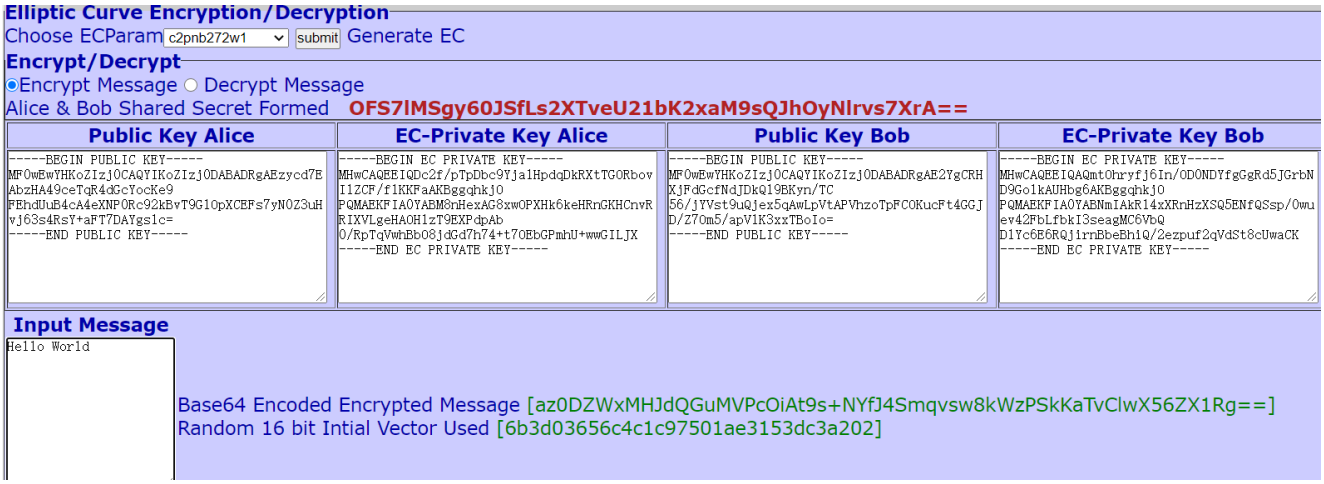
- Note:
  - The message to be sent is "Hello World".
  - Message Digest Calculator
    - Message Digest Algorithm: SHA-512
  - ECC Encryption/Decryption Tools
    - ECParam: c2pnb272w1

Ans:

Go to the online tool: https://8gwifi.org/ecfunctions.jsp

Choose the ECParam: c2pnb272w1 then click the SUBMIT bottom, we can get the Public Key and Private Keys for Alice and Bob

Alice send "Hello World" message to Bob, encrypt with Bob's public key



Base64 Encoded Encrypted Message：

az0DZWxMHJdQGuMVPcOiAt9s+NYfJ4Smqvsw8kWzPSkKaTvClwX56ZX1Rg==

Eve will receive the encrypted message from Alice but would not be able to decrypt the message because it can only be decrypted by Bob's Private Key.

After Bob received this encrypted message, he want know the content, which need to decrypting with his private key

Elliptic Curve Encryption/Decryption

Choose ECParam c2pnb272w1 submit Generate EC

Encrypt/Decrypt

Encrypt Message Decrypt Message

Alice & Bob Shared Secret Formed **OFS7lMSgy60JSfLs2XTveU21bK2xaM9sQJhOyNlrvs7XrA==**

Public Key Alice	EC-Private Key Alice	Public Key Bob	EC-Private Key Bob
-----BEGIN PUBLIC KEY----- MF0wEwYHKoZIzj0CAQYIKoZIzj0DAEADRgAEzycd7E AbzHA49ceTqR4dGcYocKe9 FEhdUuB4cA4eXNP0Rc92kBvT9G10pXCEFs7yN0Z3uH vj63s4RsY+aFT7DAYgs1c= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHwCAQEEIQDc2f/pTpDbc9Yja1HpdqDkRXtTGORbov I1ZCF/f1KKFaAKBggqhkj0 PQMAEKFIA0YAEM8nHexAG8xw0PXHk6keHRnGKHCnvR RIXVLgeHAOH1zT9EXPdpAb 0/RpTqVwhBb08jdGd7h74+t70EbGPmhU+wwGILJX -----END EC PRIVATE KEY-----	-----BEGIN PUBLIC KEY----- MF0wEwYHKoZIzj0CAQYIKoZIzj0DAEADRgAE2YgCRH XjFdGcfNdJDkQl9BKyn/TC 56/jYVst9uQjex5qAwLpVtAPVhzoTpFC0KucFt4GGJ D/Z70m5/apV1K3xxTBoIo= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHwCAQEEIQAQmtOhryfj6In/0D0NDYfgGgRd5JGrbN D9Go1kAUHbg6AKBggqhkj0 PQMAEKFIA0YABNmIAkR14xXRnHzXSQ5ENfQSsp/0wu ev42FbLfbkI3seagMC6VbQ D1Yc6E6RQjirnBbeBhiQ/2ezpuf2qVdSt8cUwaCK -----END EC PRIVATE KEY-----

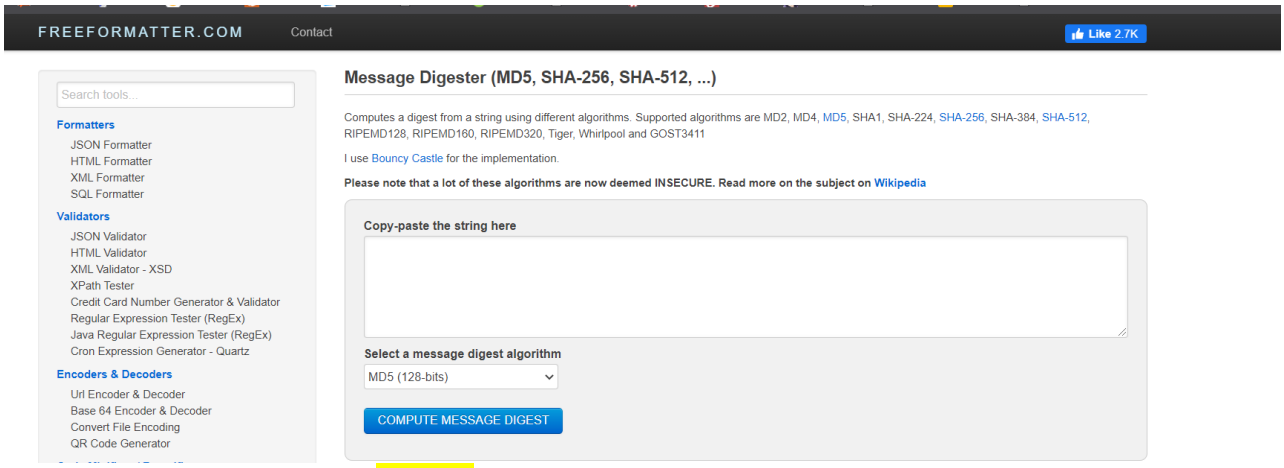
Input Message

azODZWxMHJdQGuMVPcOiAt
9s+NYfJ4SmqvsW8kWzPSkK
aTvC1wX56ZX1Rg==

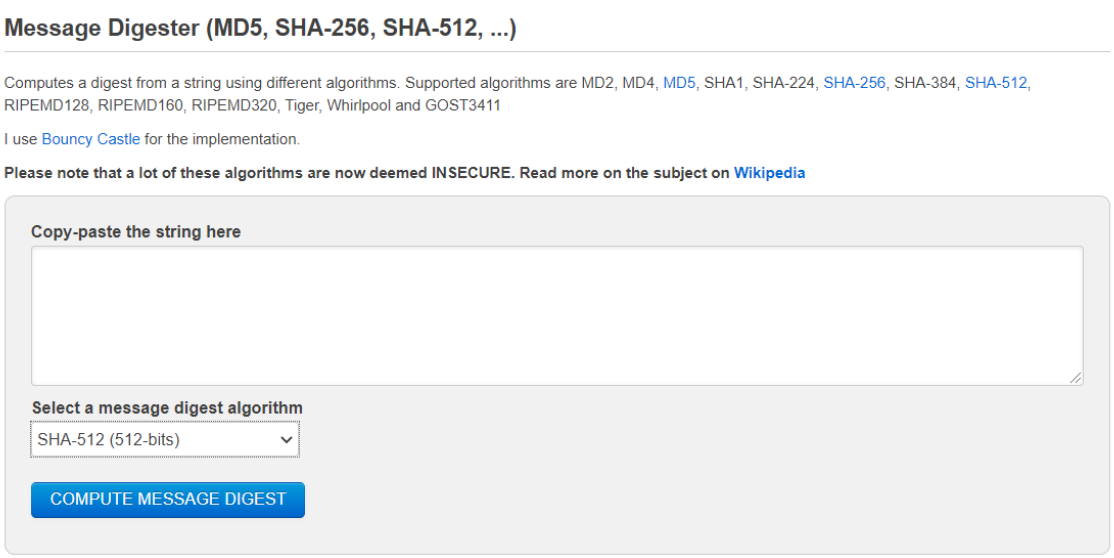
Decrypted Message [Hello World]

After decryption, Bob get Plain Message: “Hello World”

Go to Message Digest Calculator: https://www.freeformatter.com/message-digest.html

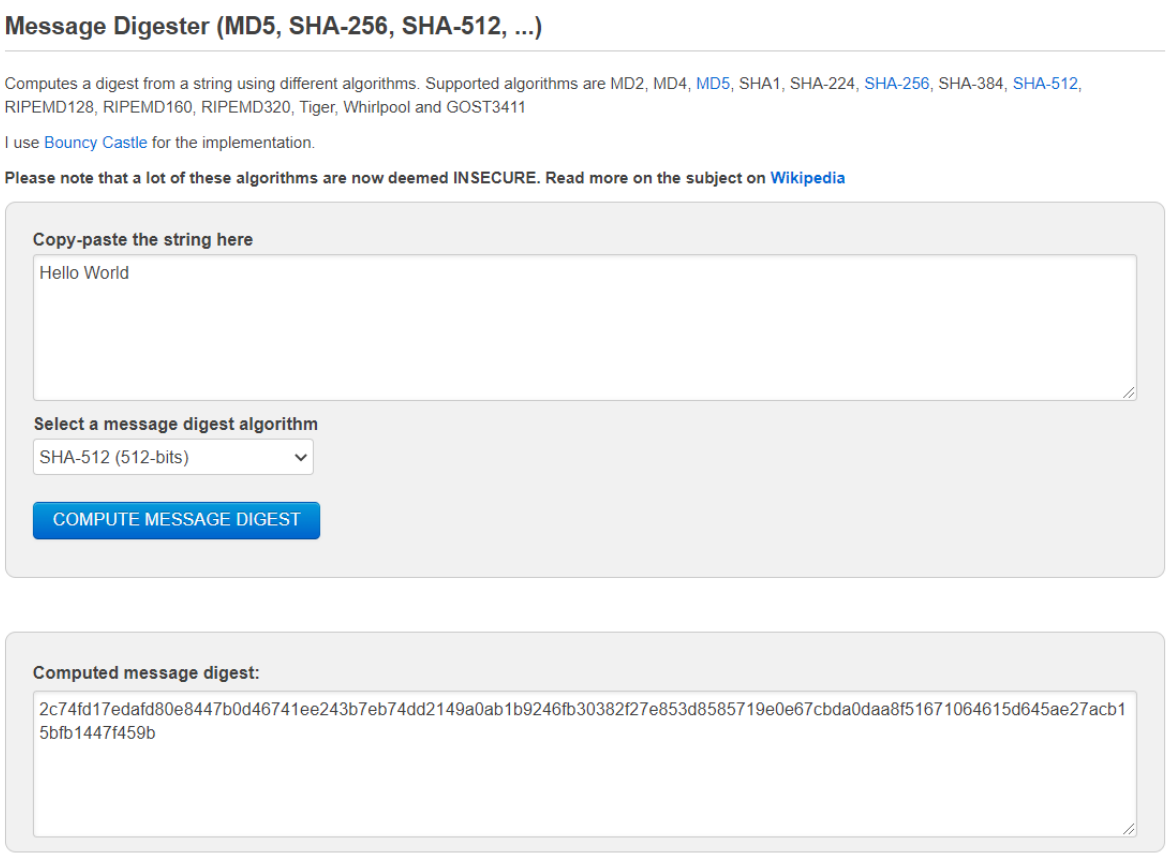


Using Message Digest Algorithm SHA-512



Enter the Alice's Plain Message "Hello World" then compute message digest:

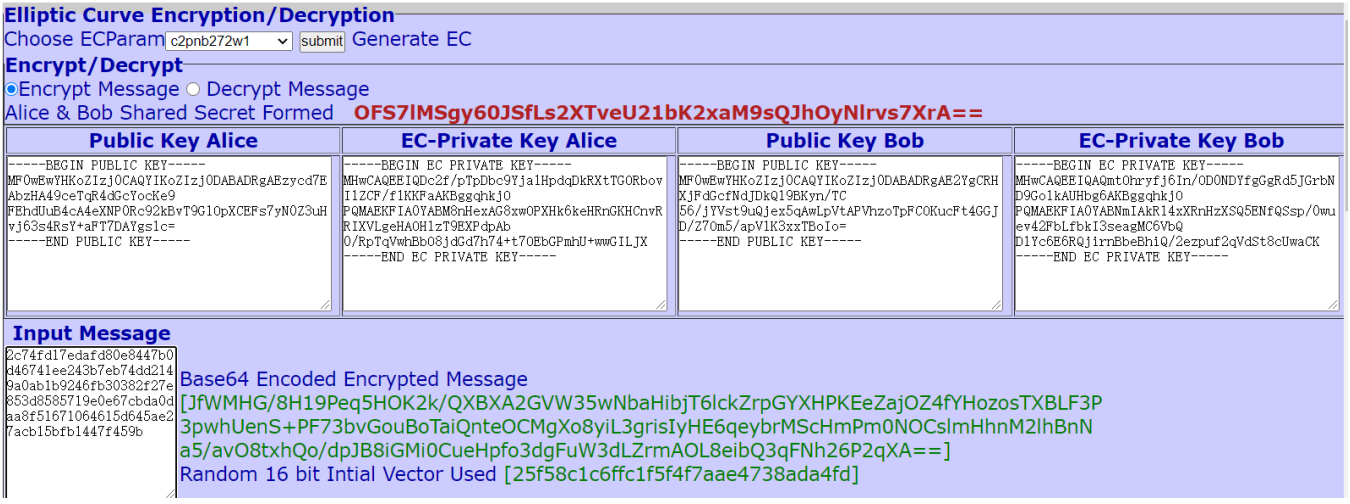
Bob also do the same thing after get the decrypted Plain Message:



Computed message digest (HASH) is:

2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b

Alice encrypt this HASH with her private key and send to Bob

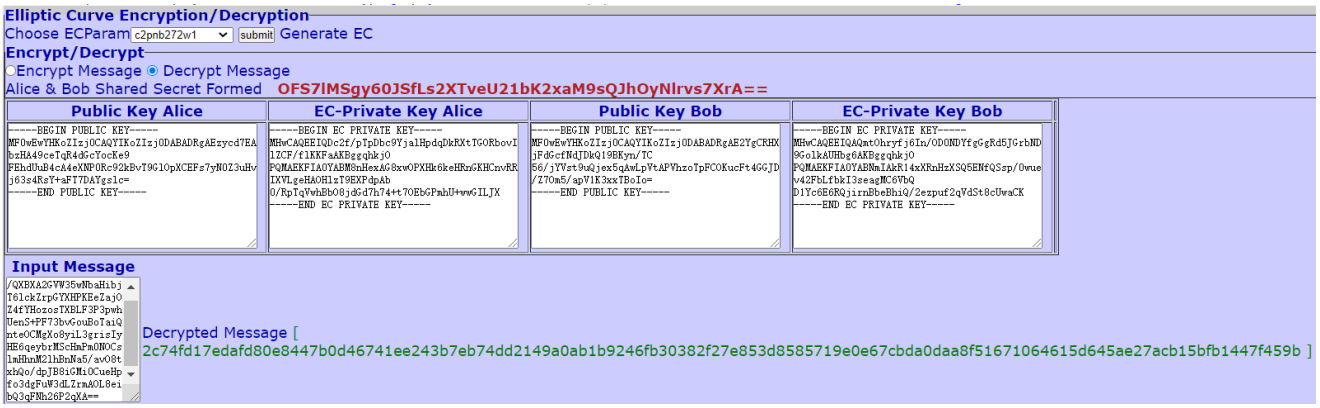


Base64 Encoded Encrypted Message:

JfWMHG/8H19Peq5HOK2k/QXBXA2GVW35wNbaHibjT6lckZrpGYXHPKEeZajOZ4fYHozosTXBLF3P 3pwhUenS+PF73bvGouBoTaiQnteOCMgXo8yiL3grisIyHE6qeybrMScHmPm0NOCslmHhnM2lhBnN a5/avO8txhQo/dpJB8iGMi0CueHpfo3dgFuW3dLZrmAOL8eibQ3qFNh26P2qXA==

Eve will receive this Encrypted message from Alice which he can verify using Alice Public key, but this will only give the HASH.

When Bob received this Encrypted Message, he need use Alice's Public Key to decrypt and get HASH



Decrypted Message:

2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b

Bob can compare those two HASH values (by Bob himself and by Alice) to see message is unchanged with same HASH values. It also proved Whitefield Diffie's Rule