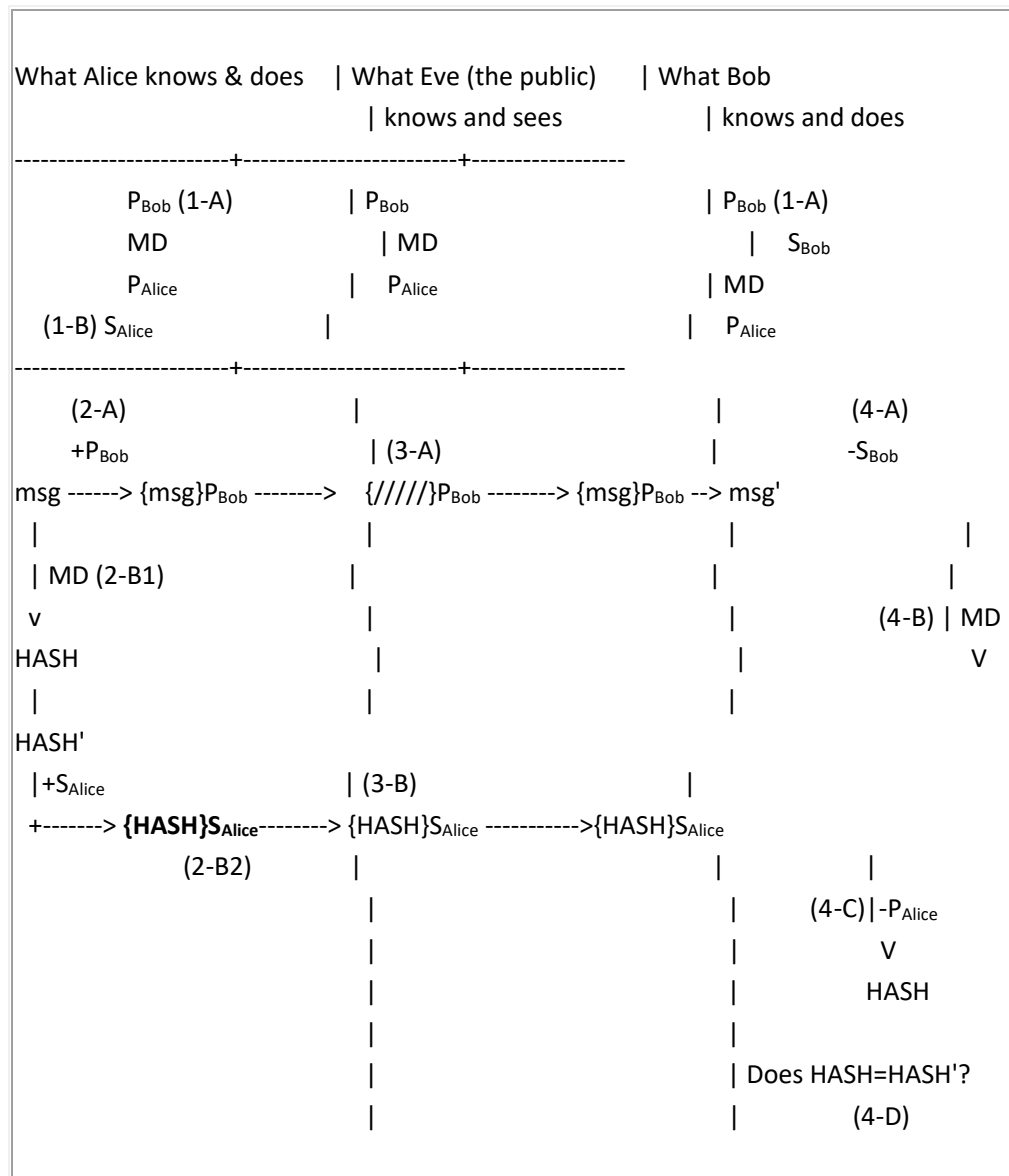


# Question:

[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](#)
    - ECParm: [c2pnb272w1](#)

Ans:

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

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

**Elliptic Curve Encryption/Decryption**  
Choose ECParm: **c2pnb272w1**  Generate EC

**Encrypt/Decrypt**  
☒ Encrypt Message ☐ Decrypt Message  
Alice & Bob Shared Secret Formed **OFS7IMSgy60JSfLs2XTveU21bK2xaM9sQJhOyNlrvs7XrA==**

Public Key Alice	EC-Private Key Alice	Public Key Bob	EC-Private Key Bob
-----BEGIN PUBLIC KEY----- MF0wEwYHkoZiZjOCAQYIKoZiZjODABADrgAEzycd7E AbzHA49ceTqR4dGcYocKc9 FEhdJub4cA4eXNP0Rc92kBVt9G10pXCEfs7yN0Z3uH vj63s4RsY+afT7DAYgs1c= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHwCAQEEIQCc2f/pTpDbc9Yja1HpdqDkRXtTGORbov I1ZCF/f1KKFAAKBggqhkj0 PQMAEKFIaOYAEM8nHexAG8xwOPXhk6keHRnGKHcnvR RIXVLgeHAOH1zT9EXPdpAb O/RpTqVwhBb08jdGd7h74+7t70EbGpmhU+wwGILJX -----END EC PRIVATE KEY-----	-----BEGIN PUBLIC KEY----- MF0wEwYHkoZiZjOCAQYIKoZiZjODABADrgAE2YgCRH XJFdGcfNdJDkQ19BKyn/TC 56/jYVst9uQJex5qAwLpVtAPVhzoTpFCOKucft4GGJ D/270m5/apV1K3xxTBoIo= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHwCAQEEIQAqmt0hryfj6In/ODONDYfgGgRd5JGrbN D9Go1kAUHbg6AKBggqhkj0 PQMAEKFIaOYAEM8nIAkR14xXRnHzXSQ5ENfQSSp/OwU ev42FbLfbkI3seagMC6VbQ D1Yc6E6RQj1rrBbeBh1Q/2ezpuf2qVdSt8cUwaCK -----END EC PRIVATE KEY-----

**Input Message**  
Type Something Here...

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

**Elliptic Curve Encryption/Decryption**  
Choose ECParm: **c2pnb272w1**  Generate EC

**Encrypt/Decrypt**  
☒ Encrypt Message ☐ Decrypt Message  
Alice & Bob Shared Secret Formed **OFS7IMSgy60JSfLs2XTveU21bK2xaM9sQJhOyNlrvs7XrA==**

Public Key Alice	EC-Private Key Alice	Public Key Bob	EC-Private Key Bob
-----BEGIN PUBLIC KEY----- MF0wEwYHkoZiZjOCAQYIKoZiZjODABADrgAEzycd7E AbzHA49ceTqR4dGcYocKc9 FEhdJub4cA4eXNP0Rc92kBVt9G10pXCEfs7yN0Z3uH vj63s4RsY+afT7DAYgs1c= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHwCAQEEIQCc2f/pTpDbc9Yja1HpdqDkRXtTGORbov I1ZCF/f1KKFAAKBggqhkj0 PQMAEKFIaOYAEM8nHexAG8xwOPXhk6keHRnGKHcnvR RIXVLgeHAOH1zT9EXPdpAb O/RpTqVwhBb08jdGd7h74+7t70EbGpmhU+wwGILJX -----END EC PRIVATE KEY-----	-----BEGIN PUBLIC KEY----- MF0wEwYHkoZiZjOCAQYIKoZiZjODABADrgAE2YgCRH XJFdGcfNdJDkQ19BKyn/TC 56/jYVst9uQJex5qAwLpVtAPVhzoTpFCOKucft4GGJ D/270m5/apV1K3xxTBoIo= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHwCAQEEIQAqmt0hryfj6In/ODONDYfgGgRd5JGrbN D9Go1kAUHbg6AKBggqhkj0 PQMAEKFIaOYAEM8nIAkR14xXRnHzXSQ5ENfQSSp/OwU ev42FbLfbkI3seagMC6VbQ D1Yc6E6RQj1rrBbeBh1Q/2ezpuf2qVdSt8cUwaCK -----END EC PRIVATE KEY-----

**Input Message**  
Hello World

Base64 Encoded Encrypted Message [az0DZWxMHJdQGUMVPcOiAt9s+NYfJ4SmqvsW8kWzPSKkaTvClwX56ZX1Rg==]  
Random 16 bit Initial Vector Used [6b3d03656c4c1c97501ae3153dc3a202]

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   Generate EC

### Encrypt/Decrypt

☐ Encrypt Message ☒ Decrypt Message

Alice & Bob Shared Secret Formed **OFS7IMSGy60JSfLs2XTVeU21bK2xaM9sQJhOyNlrvs7XrA==**

Public Key Alice	EC-Private Key Alice	Public Key Bob	EC-Private Key Bob
-----BEGIN PUBLIC KEY----- MF0wEwYHkoZIZjOCAQYIKoZIZjODABADrgABZyCd7B AbzHA49ceTqR4dGcYocke9 FhduUB4cA4eXNPORc92kByT9G1OpXCEFs7yN0Z3uH vj63s4rSt+aPT7DAYs1c= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHwCAQEEIQCc2f/pTpDbc9Yja1HpdqDkRXtTGORbov I1ZCF/f1KKPaAKBggqhkjO PQMAEKFAOYAEM8nHexAG8xwOPXhk6keHRnGKHcnvR RIXVLgeHAOH1zT9EXFPdpAb 0/RpTqVwhBb08jdGd7h74+t70EbGpmbU+wwGILJX -----END EC PRIVATE KEY-----	-----BEGIN PUBLIC KEY----- MF0wEwYHkoZIZjOCAQYIKoZIZjODABADrgAB2YgCRH XjFgGcfNdJdkQ19BKyn/TC 56/jYVst9uQjex5qAwLpVtAPVhzoTpFCOKucPt4GGJ D/Z70m5/apV1K3xxTBoIo= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHwCAQEEIQAQmt0hryyfj6In/ODONDYfgGgRd5JGrbN D9G01kAUHbg6AKBggqhkjO PQMAEKFAOYAENmLAKR14zXRnHzXSQ5ENfQSSp/0wu ev42FbLfokI3seagMC6VbQ D1Yc6B6RqjirmBbeBhiQ/2ezpuf2qVdSt8cUwaCK -----END EC PRIVATE KEY-----

### Input Message

sz0DZWwMHjdGGuMVPc01At  
0e+NYfj4Smqzsw8kWzPskk  
aT+C1wX56ZK1Rg==

Decrypted Message [ Hello World ]

After decryption, Bob get Plain Message: **"Hello World"**

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

FREEFORMATTER.COM

Contact

Like 2.7K

Search tools...

Formatters

JSON Formatter

HTML Formatter

XML Formatter

SQL Formatter

Validators

JSON Validator

HTML Validator

XML Validator - XSD

XPath Tester

Credit Card Number Generator & Validator

Regular Expression Tester (RegEx)

Java Regular Expression Tester (RegEx)

Cron Expression Generator - Quartz

Encoders & Decoders

Uri Encoder & Decoder

Base 64 Encoder & Decoder

Convert File Encoding

QR Code Generator

Message Digester (MD5, SHA-256, SHA-512, ...)

Computes a digest from a string using different algorithms. Supported algorithms are MD2, MD4, MD5, SHA1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD128, RIPEMD160, RIPEMD320, Tiger, Whirlpool and GOST3411

I use Bouncy Castle for the implementation.

Please note that a lot of these algorithms are now deemed INSECURE. Read more on the subject on Wikipedia

Copy-paste the string here

Select a message digest algorithm

MD5 (128-bits)

COMPUTE MESSAGE DIGEST

Using Message Digest Algorithm **SHA-512**

### Message Digester (MD5, SHA-256, SHA-512, ...)

Computes a digest from a string using different algorithms. Supported algorithms are MD2, MD4, MD5, SHA1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD128, RIPEMD160, RIPEMD320, Tiger, Whirlpool and GOST3411

I use Bouncy Castle for the implementation.

Please note that a lot of these algorithms are now deemed INSECURE. Read more on the subject on Wikipedia

Copy-paste the string here

Select a message digest algorithm

SHA-512 (512-bits)

COMPUTE MESSAGE DIGEST

Enter the Alice’s Plain Message “Hello World” then compute message digest:  
Bob also do the same thing after get the decrypted Plain Message:

Message Digester (MD5, SHA-256, SHA-512, ...)

Computes a digest from a string using different algorithms. Supported algorithms are MD2, MD4, MD5, SHA1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD128, RIPEMD160, RIPEMD320, Tiger, Whirlpool and GOST3411

I use Bouncy Castle for the implementation.

Please note that a lot of these algorithms are now deemed INSECURE. Read more on the subject on Wikipedia

Copy-paste the string here

Hello World

Select a message digest algorithm

SHA-512 (512-bits)

COMPUTE MESSAGE DIGEST

Computed message digest:

2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b

Computed message digest (HASH) is:  
2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b

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

Elliptic Curve Encryption/Decryption

Choose ECParmc2pnb272w1submitGenerate EC

Encrypt/Decrypt

☒ Encrypt Message ☐ Decrypt Message

Alice & Bob Shared Secret FormedOFS7IMSgy60JSfLs2XTVeU21bK2xaM9sQJhOyNlrvs7XrA==

Public Key Alice	EC-Private Key Alice	Public Key Bob	EC-Private Key Bob
-----BEGIN PUBLIC KEY----- MF0mEwYHkoZlZjOCAQYIKoZlZjODABADRgAEzycd7E AbzHA49ceTqR4dGcYoCke9 FEhJluB4cA4eXMPORc92kbvT9G10pXCEFS7yN0Z3uH vj63s4RsY+aFT7DAygs1c= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHwCAQEEIQCc2f/pTpDbc9Yj1aHpdqDkRXtTGORbov I1ZCF/f1KKFaAKBgqhkj0 PQMAEKFAOYABM8nHexAG8xwOPXHk6keHRnGKHcnvR R1XVLeeHA0H1zT9EXPdpAb O/RpTqVwhBb08jdGd7h74+t70EtCPmhU+wwGILJX -----END EC PRIVATE KEY-----	-----BEGIN PUBLIC KEY----- MF0mEwYHkoZlZjOCAQYIKoZlZjODABADRgAE2YgCRH XjPdGcfNqJdkQ19BKyn/TC 56/jYVst9uQjex5qAwLpVtAPVnzoTpFCOKucFt4GGJ D/270m5/apV1K3xxTBoIo= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHwCAQEEIQAQmt0hryfj6In/ODONDYfgGgRd5JGrbN D9Go1kAUHbg6AKBgqhkj0 PQMAEKFAOYABM8nHexAG8xwOPXHk6keHRnGKHcnvR R1XVLeeHA0H1zT9EXPdpAb O/RpTqVwhBb08jdGd7h74+t70EtCPmhU+wwGILJX -----END EC PRIVATE KEY-----

Input Message

2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b

Base64 Encoded Encrypted Message

[JfWMHG/8H19Peq5HOK2k/QXBXA2GVW35wNbaHibjT6lckZrpGYXHPKEEzajOZ4fyHozosTXBLF3P3pwhUenS+PF73bvGouBoTaiQnteOCMgXo8yiL3grisIyHE6qeybrMSchMpm0NOCslmHhnM2lhBnNa5/avO8txhQo/dpJB8iGMi0CueHpfo3dgFuW3dLZrmaOL8eibQ3qFNh26P2qXA==]

Random 16 bit Intial Vector Used [25f58c1c6ffc1f5f4f7aae4738ada4fd]

Base64 Encoded Encrypted Message:  
JfWMHG/8H19Peq5HOK2k/QXBXA2GVW35wNbaHibjT6lckZrpGYXHPKEEzajOZ4fyHozosTXBLF3P3pwhUenS+PF73bvGouBoTaiQnteOCMgXo8yiL3grisIyHE6qeybrMSchMpm0NOCslmHhnM2lhBnNa5/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

**Elliptic Curve Encryption/Decryption**  
Choose ECParam: c2pnb272w1 [submit] Generate EC

**Encrypt/Decrypt**  
☐ Encrypt Message ☒ Decrypt Message  
Alice & Bob Shared Secret Formed: **OFS7IMSGy60JSfLs2XTveU21bK2xaM9sQJhOyNlrvs7XrA==**

Public Key Alice	EC-Private Key Alice	Public Key Bob	EC-Private Key Bob
-----BEGIN PUBLIC KEY----- MF0wEwYHKOZIsjOCAYIKoZIsjODABADRAEzycd7EA bzHA49ceTqR495cYocRe9 PEhd0b4c44eXNPUrc92k8vT9610pXCEPse7yN0Z3uRv j63s4RzF7sFTTAAZg1c= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MhwCAQEIEIQc2t/pTpDbc9Vj1HpdqBkRXtT6ORb0vI LZCF/t1KKFaaKBeggqbkj0 PQMAEKFIAUTAB8nHoxA68xwOPXHB6keHbzEHCnVRK IXVtgcHAGH1sT9EXPdpAb 0/RpTgVvbB08j95d7h74+70EbGpmbJ+vv6ILJX -----END EC PRIVATE KEY-----	-----BEGIN PUBLIC KEY----- MF0wEwYHKOZIsjOCAYIKoZIsjODABADRAE2YgCRHX jF6gcFRdJdk198Eyn/TC S6/jYvt9uqjex5qwlP*APVhzoTpFC0KucFt46GJD /Z70m5/spYIK3xxTBoIc= -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MhwCAQEIEIQAmT0hryfj61n/ODONDYfg5gRd5JGcrND 96o1kAUHb6GAKEggqbkj0 PQMAEKFIAUTAB8nHoxA68xwOPXHB6keHbzEHCnVRK IXVtgcHAGH1sT9EXPdpAb 0/RpTgVvbB08j95d7h74+70EbGpmbJ+vv6ILJX -----END EC PRIVATE KEY-----

**Input Message**  
/QXBXA2GVW35WbHaHibj  
T61ckZrp6YXHPKEeZaj0  
Z4tYHozosIXGLF3P3pwh  
UenS+FE73bvGouBoFaiq  
nte0CMgXo8yil3grizly  
HE6qeybtrN5cHmPmONOCs  
1n0bnM21hBnNa5/av08t  
xh4co/dpJBS10R10cuesp  
fo3dgFuW3dLzrm8OL8ei  
bQ3qFh26F2qXA==

**Decrypted Message [**  
**2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b ]**

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