# Cryptography Lab
# Weeks 11-20 Outputs

Shivangi Narayan

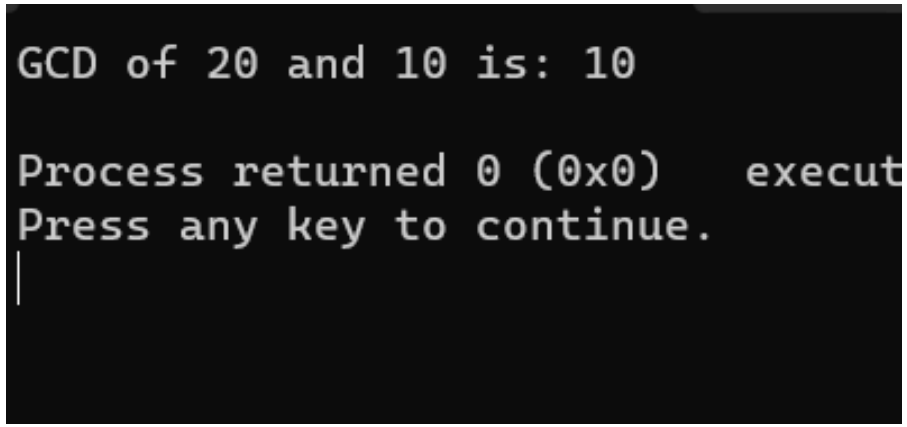
AP211100010469

# Week 11

```
Encrypted Message: ttnaaptmtsuoaodwcoixknlypetz
Decrypted Message: attackpostponeduntiltwoamxyz

Process returned 0 (0x0)   execution time : 0.122 s
Press any key to continue.
```

# Week 12


GCD of 20 and 10 is: 10
Process returned 0 (0x0)   execut
Press any key to continue.

# Week 13

```
>>
========================================= RESTART: C:/U
Key provided: 0f1571c947d9e8590cb7add6af7f6798
Keywords:

w0 = 0f 15 71 c9
w1 = 47 d9 e8 59
w2 = 0c b7 ad d6
w3 = af 7f 67 98
w4 = dc 90 37 b0
w5 = 9b 49 df e9
w6 = 97 fe 72 3f
w7 = 38 81 15 a7
w8 = d2 c9 6b b7
w9 = 49 80 b4 5e
w10 = de 7e c6 61
w11 = e6 ff d3 c6
w12 = c0 af df 39
w13 = 89 2f 6b 67
w14 = 57 51 ad 06
w15 = b1 ae 7e c0
w16 = 2c 5c 65 f1
w17 = a5 73 0e 96
w18 = f2 22 a3 90
w19 = 43 8c dd 50
w20 = 58 9d 36 eb
w21 = fd ee 38 7d
w22 = 0f cc 9b ed
w23 = 4c 40 46 bd
w24 = 71 c7 4c c2
```

```
w22 = 0f cc 9b ed
w23 = 4c 40 46 bd
w24 = 71 c7 4c c2
w25 = 8c 29 74 bf
w26 = 83 e5 ef 52
w27 = cf a5 a9 ef
w28 = 37 14 93 48
w29 = bb 3d e7 f7
w30 = 38 d8 08 a5
w31 = f7 7d a1 4a
w32 = 48 26 45 20
w33 = f3 1b a2 d7
w34 = cb c3 aa 72
w35 = 3c be 0b 38
w36 = fd 0d 42 cb
w37 = 0e 16 e0 1c
w38 = c5 d5 4a 6e
w39 = f9 6b 41 56
w40 = b4 8e f3 52
w41 = ba 98 13 4e
w42 = 7f 4d 59 20
w43 = 86 26 18 76
>
```

# Week 14

```
e. AES Encryption
d. AES Decryption

n. Exit
--Choice : e

<-------->
Enter Plain Text String (16-bits) : HelloWorldCrypto

Enter Key String (16-bits) : abcdabcdabcdabcd

AES ENCRYPTION DONE :
:::::=> Plain Text (input) : HelloWorldCrypto
:::::=> Key0 (input) : abcdabcdabcdabcd        :::=> Key1 : 1111111111111111   :::=> Key2  : 1011100001000111
:::::=> Cipher Text (output) : 1110110100010010



e. AES Encryption
d. AES Decryption

n. Exit
--Choice : d

<-------->
Enter Cipher Text String : 1110110100010010

Enter Key String (16-bits) : abcdabcdabcdabcd

AES DECRYPTION DONE :
:::::=> Cipher Text (input) : 1110110100010010
:::::=> Key0 (input) : abcdabcdabcdabcd        :::=> Key1 : 1111111111111111   :::=> Key2  : 1011100001000111
:::::=> Plain Text (output) : 1111111111111111
```

# Week 15

```
PS C:\Users\Shivangi\Desktop\JavaCode> java .\Cry15.java
Your Key-1 :
1 0 1 0 0 1 0 0
Your Key-2 :
0 1 0 0 0 0 1 1
Your plain Text is :
1 0 0 1 0 1 1 1
Your cipher Text is :
0 0 1 1 1 0 0 0
Your decrypted Text is :
1 0 0 1 0 1 1 1
PS C:\Users\Shivangi\Desktop\JavaCode>
```

# Week 16

```
100 3 231 14 19 26 44 48 159 101 83 164 81 120 123 144
161 196 31 153 179 230 24 200 74 110 67 146 140 130 237 136
208 86 0 135 172 4 238 244 82 34 58 132 96 225 186 155
192 28 209 80 46 212 9 87 38 127 60 72 188 121 133 202
247 151 147 246 255 11 165 242 125 77 33 99 118 134 199 207
214 221 177 160 107 119 218 50 27 61 253 71 239 141 175 236
106 205 92 194 1 174 7 84 114 137 22 95 193 163 16 191
204 185 49 116 20 62 216 189 47 162 54 250 18 90 124 79
56 198 112 166 217 206 167 154 122 170 203 143 173 156 240 152
171 138 15 13 248 41 5 97 226 234 150 142 117 35 108 57
91 103 235 158 64 75 42 145 29 70 190 243 109 17 25 126
201 43 169 232 32 115 184 59 183 63 102 69 168 233 223 36
6 66 52 157 213 55 139 93 210 182 228 254 40 78 176 129
2 131 53 76 30 215 219 241 104 113 222 148 111 249 245 128
37 23 51 229 88 195 12 187 197 94 211 251 65 149 252 8
227 180 178 98 45 224 220 85 89 73 10 39 21 181 105 68

Keys for plaintext: 196 102 226 189 141 131 159 206 142 103 141 206
Message: cryptography
Encrypted Message:  °¢═•∞°╝∩σ╖
Decrypted Message:  cryptography
```

```
91 40 23 132 215 207 65 81 17 110 216 237 165 173 248 219
240 247 208 177 87 149 145 236 185 217 76 107 79 100 138 174
190 155 89 30 214 71 239 212 108 202 99 135 160 104 27 66
184 21 106 1 26 161 143 221 251 90 82 224 3 57 10 200
133 246 19 121 63 195 88 169 86 73 117 201 220 9 196 24
8 127 25 95 142 77 20 12 103 115 189 176 34 37 134 53
58 22 33 101 78 126 232 137 197 84 41 250 150 254 0 205
222 153 62 139 170 255 2 171 226 11 249 218 199 154 122 213
141 18 159 151 130 233 113 59 5 253 55 163 210 4 158 157
203 243 111 83 93 242 188 168 180 15 223 241 198 191 72 38
112 105 125 120 182 75 175 85 231 172 14 166 116 192 238 167
124 181 209 140 245 229 162 48 119 64 94 36 179 178 211 102
28 7 187 118 29 206 49 109 194 228 96 97 44 42 47 51
123 146 13 114 43 92 98 252 50 45 70 31 56 52 39 152
227 46 244 131 61 32 183 67 54 144 225 164 156 148 128 235
230 60 129 234 16 35 186 6 69 147 80 74 204 68 136 193

Keys for plaintext: 93 152 80 162 30
Message: SRMAP
Encrypted Message: ╩πN
Decrypted Message: SRMAP
```

# Week 17

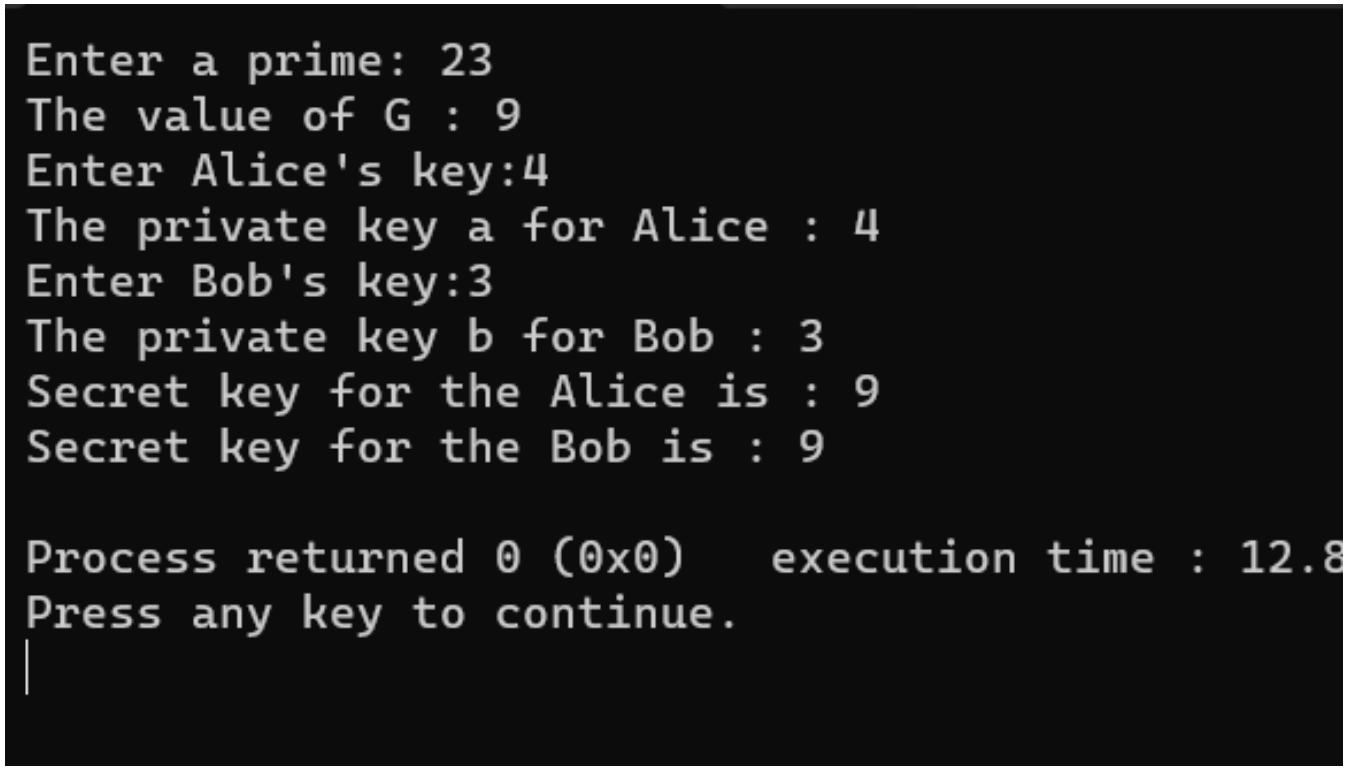
```
enter the message
Cryptocurrency
Initial message:
Cryptocurrency

The encoded message(encrypted by public key)
642134934279554701689232420161349134914271623243427

The decoded message(decrypted by private key)
Cryptocurrency

Process returned 0 (0x0)   execution time : 8.829 s
Press any key to continue.
```

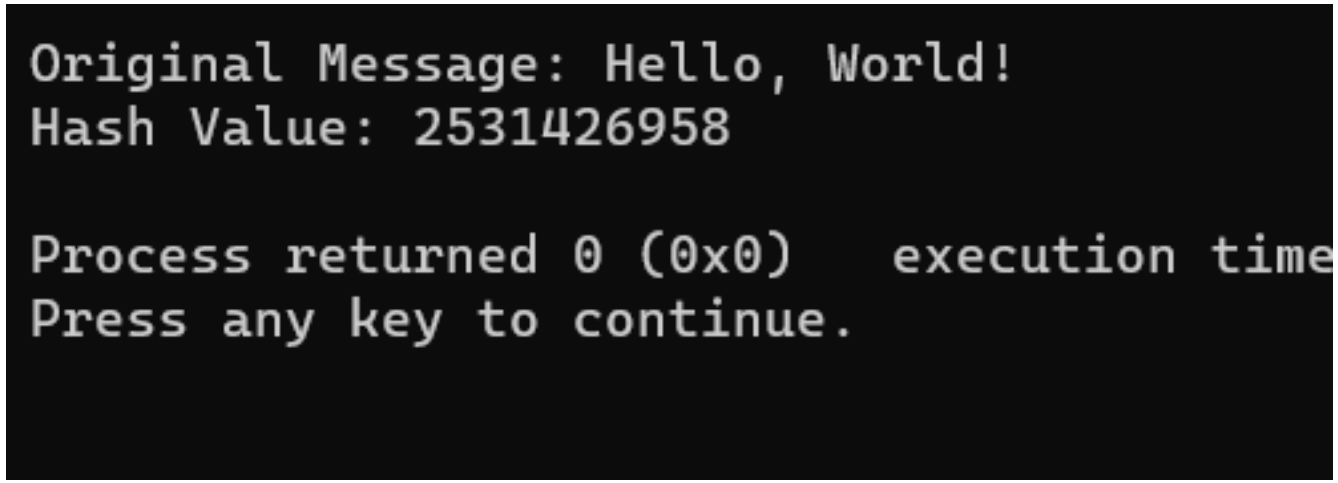
# Week 18


Enter a prime: 23
The value of G : 9
Enter Alice's key:4
The private key a for Alice : 4
Enter Bob's key:3
The private key b for Bob : 3
Secret key for the Alice is : 9
Secret key for the Bob is : 9
Process returned 0 (0x0) execution time : 12.8
Press any key to continue.

# Week 19

```
>>>
== RESTART: C:/Users/Shivangi/AppData/Local/Programs/Python/Python310/Cry19.py =
X: 0x3abd423dc939f480ac9ad328e90e09e84d92dae80bdf8500add36956b945a880
Y: 0x678117888a66df1a89a5412a2fa4d6131ab1987e93288d11f44c8c20639aa90b1
Currently exchange the publickey (e.g. through Internet)
A shared key : 0x75d8615c776be92c4ffdc9607d2b67f90eb5d618cb87e64ad151e63f1650be611
(B) shared key : 0x75d8615c776be92c4ffdc9607d2b67f90eb5d618cb87e64ad151e63f1650be611
Equal shared keys: True
>>>
```

# Week 20


Original Message: Hello, World!
Hash Value: 2531426958
Process returned 0 (0x0)   execution time
Press any key to continue.