# ElGamal Encryption 과제

# ElGamal Encryption

$(G, p, g) \leftarrow Gen(1^k)$
$x \leftarrow^{\$} Z_p, \quad y = g^x$
$PK = (G, p, g, y)$
$SK = x$

$PK$

$CT$

$Enc_{PK}(m)$:
$r \leftarrow^{\$} Z_p$
$CT = < g^r, m \cdot y^r >$

$Dec_{SK}(CT)$:
$C1, C2 \leftarrow CT$
$m = \frac{C2}{C1^x}$

Setup :

p ← random 1024 bit safe prime

g (p의 generator)

$x \leftarrow Z_p$

$y = g^x \bmod p$

pub = (p,g,y)

priv = x

Enc(m, pub) :

$r \leftarrow Z_p$

$c_1 = g^r \bmod p$

$c_2 = m \cdot y^r \bmod p$

Dec(C, priv, pub) :

$C = (c_1, c_2)$

$m = \frac{c_2}{c_1^x} \bmod p$ <- $c_2$와 $c_1^x$의 inverse(mod p 에 대한) 를 곱하면 됩니다.

$= c_2 * inv(c_1^x) \bmod p$

## 출력 예시

```
Complete the select of prime
Complete the select of generator
p       : D12703B1A92B37282D9A91EEF9EA2375E5EAAC606023057F71BA8BBE3C062CFB20
ACE2DDCBCB359E2F6068384D98F75A1499D060E5A6BF708194224E66C5B626DA79F98C93FD37
0E204E2221565041CA776D3E3334A590FD8EA5EC1B82C8561ADA3BC50A3AD12DC386751334A1
6AA0115678D99EB9B917E2FB66B17D8BBD7005
g       : B3D2C62D5A1A608D8CC4F852AAB24C87680E0CF0227A818C4618FCD48722D08BCB
9A7B47146DBE2FAEA1F7D16ED198A2C8AB3ABCC464E186100F8441C483A48A2874D40B7A0DB5
5ACC9588DA37E4736AED8FDBF65C05599C1A9A46D996BED269F335242EE663F3688A6AF7B742
290AC101A57F74570E64B85F1C5C134BE50770
c1      : 0E91B030D547C7CC65E2D44B55BB5315B1C4894088F85AF6BE007DEBB083530093
68D15C7BD897CFE768BA207E228DE145CE746781A04D39F9A6543C1FD131381B20C60152AC74
B81A5C97E2D612DD9054343F0041F126CB4F30C12E73B5DC39861FD53BB470B06D10A985E05D
BB838BB7A51F858A8A4886F637D9B47BAC4F9A
c2      : 83135521C9DFC4FAC94EF87CC582165F2CAF7ADA5E51552957411E8A9DFFD76AEB
794960CCE298937F9933FFD2EBCAC442EB84A6484B54B7B4C838FDD908FE46B330E02B0DF268
4D57699CA684FF5733FA2962FAD67FCE55CDDAF446D7DAD180C36FEE3D26F62704FA854C86D7
60CBBD4EC056E124C6BCA1D75B33CA4F22FAEB
dec     : hello, world
msg_len : 12
```

※실행이 수 초간 소요될 수 있음

# RSA 과제

KeyGen

p, q : pick 1024 bits prime

N = p*q

φ(N) = (p-1)*(q-1)

e : pick random number(3으로 고정)

d : inverse e

pk := (N,e)

sk := d

return (N, e, d)

Enc(m,pk)

c = $m^e$ mod n

return c

Dec(c,sk)

m = $c^d$ mod n

return m

<Inverse e 구하는 방법>

단, e 와 φ(N)는 서로소

Ext-Euclid(e, φ(N)) = (1,x',y')

d = x' mod φ(N)

※

(e * d + φ(N)*y') mod φ(N) = 1 mod φ(N)

# RSA 출력 결과

```
e        : 03
N        : E56777F3838C2A73DCF675521588322B737966F7A35BF877C339302148D9D5A3F45684F1F09751EC9840111F0182BE5348E7B61AF
050D563F7D4F6FABAC7C10489CC21238DAA165AF002541FDF75D13BF3F755DB6E9DC53F11DF69A4509F0713DF2AC99298C22B54AAD25F28187B0
4776DE7F53D35D8D9E527F3BCD77A57A341A9D79A6EEB5EBEC76B73ADD026523380FEA9CC58E29FDAA7191549FECB70A889DB5B29F8130A95CD7
C4D99762C3FB12D3B9B275E0E635EEAD1A0E55175880F5FB3A0DCE668D721421AEDB61F083AD317A54A6693BA715B17FCA29D7E2F6B634F09DCF
9B5B98792D31568CD6075CB4D88F67F37B7E4EE3A224FAC6D98CEAB7615
dxy.y    : 98EFA54D025D71A2934EF8E163B021724CFB99FA6CE7FAFA8226201630913917F839ADF6A064E14865800B6A0101D43785EFCEBCA
035E397FA8DF9FC7C852B585BDD6B6D091C0EE74AAC38153FA3E0D2A2A4E3E79F13D8D4B694F11835BF5A0D3F71DBB71081723871E194C565A75
84F9E9AA37E23E5E698C54D288FA6E5177FD887A5C22435F1547A5182F0223EEE5FE6042AF2D5488A9B7D718485C8F15BC207CE7535FC65AC10E
8DE96ACC6C6EA60681B814AC7E46BD42C856552C0FA460E926DA9C2FC66130702E5A1926E2AABADA118CA927CE18E2A5E68181569229D6938414
7BB5438229A0F513BE49F19A1E585000B7BF0A9DA1CC4129394C285BEB3
dxy.x    : 01
dxy.d    : 01

Cipher text : 115C68778FF822C0F50BF5F76BE870948000
dec : hello
```