4

2.8

Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communications using the El-Gamal public key cryptosystem.

a

Alice's private key is $a = 947$. What is her public key A?

✓ **Answer**

$A \equiv g^a \mod p$

$A \equiv 177$

b

Bob has private key $b = 716$ and public key $B = 469$. Alice encrypts message $m = 583$ with nonce $k = 877$. What ciphertext does she send to Bob?

✓ **Answer**

$c_1 = g^k \mod p = 719$

$c_2 = mB^k = 1296$

$c = (719, 1296)$

c

Alice gets new private key $a = 299$ and public key $A = 34$. Bob sends message $(661, 1325)$ using this new public key. Decrypt the message.

✓ **Answer**

$x = c_1^{p-1-a} = 794$

$m = c_2 x = 332$

332

d

Bob has new public key $B = 893$. Alice sends him the message $(693, 793)$. Eve manages to solve the discrete log problem(with generous assistance from you) and uses b to decrypt the message. What is the message?

✓ **Answer**

$k = 932$

$A^k = 431$

$A^{-k} = 532$

$m = 365$