

Course > Week 4 > Home... > Home...

Homework 4

☐ Bookmark this page

Homework 4-1

2/2 points (graded)

Today, several cryptosystems using prime numbers have been proposed. Choose the cryptosystem for which exponentiation \pmod{P} is used to encrypt messages, and its security is based on the hardness of the Discrete Logarithm Problem.

- The Diffie-Hellman Key Exchange
- The RSA Cryptosystem
- The ElGamal Encryption System
- The Miller-Koblitz Elliptic Curve Cryptosystem

Submit

✓ Correct (2/2 points)

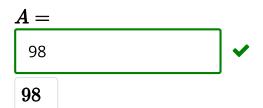
Homework 4-2-1

1/1 point (graded) Let $m{A}$ be the integer $m{A}$ satisfying $2^{63} \equiv A \pmod{131}$ and $0 \leq A \leq 130$.

Let \boldsymbol{B} be the minimum positive integer satisfying

$$3^B \equiv 26 \pmod{31}$$
.

Find A.



Submit

✓ Correct (1/1 point)

Homework 4-2-2

1/1 point (graded)

Let A be the integer A satisfying

$$2^{63} \equiv A \pmod{131}$$
 and $0 \leq A \leq 130$.

Let $oldsymbol{B}$ be the minimum positive integer satisfying

$$3^B \equiv 26 \pmod{31}$$
.

Find $oldsymbol{B}$.

Submit

✓ Correct (1/1 point)

Homework 4-3

2/2 points (graded)

Consider the RSA cryptosystem with parameter N=65 and (public) encryption key E=11. What is the decryption key $m{D}$ for this cryptosystem?



? Hint (1 of 1): factorize N.

Next Hint

Submit

✓ Correct (2/2 points)

Homework 4-4

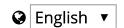
2/2 points (graded) The elliptic curve

$$Y^2 = X^3 + 2$$

has six **mod** 5 points including the point at infinity. Five of them are ∞ , (2,0), (3,3), (4,1), (4,4). Find the sixth **mod** 5 point (S,T).







© 2012–2017 edX Inc. All rights reserved except where noted. EdX, Open edX and the edX and Open edX logos are registered trademarks or trademarks of edX Inc. | 粤ICP备17044299号-2













