



Course > Week 4 > Prime ... > Proble...

Problem (5-6)

🔖 Bookmark this page

Problem 5

1/1 point (graded)

The RSA cryptosystem is the first practical public key cryptosystem invented in 1978.

Choose the correct statement.

- ☐ The RSA cryptosystem is named after Riemann, Socrates, and Aristotle.
- ☐ The RSA cryptosystem is very secure because its security was rigorously proved by Reciprocity Laws on prime numbers.
- ☒ The security of the RSA cryptosystem was not yet rigorously proved. People believe the RSA cryptosystem is probably secure because factoring a given integer seems a computationally hard problem. ✓
- ☐ Because the computer technology is highly developed, it is very easy to attack the RSA cryptosystem today. By that reason, the RSA cryptosystem is not used any more today.

Submit

You have used 1 of 2 attempts

i Answers are displayed within the problem

Problem 6

1/1 point (graded)

Consider the RSA cryptosystem with parameter $N = 55$, encryption (public) key $E = 7$, and decryption key $D = 23$. Assume that the plaintext is $X = 9$. Find the ciphertext Y .

(Note that Y is an integer satisfying $0 \leq Y \leq N - 1$ and $Y \equiv X^E \pmod{N}$)

$Y =$

✓ Answer: 4

Submit

You have used 1 of 2 attempts

i Answers are displayed within the problem

[Learn About Verified Certificates](#)

© All Rights Reserved



 English ▼

© 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

POWERED BY
OPENedX

