МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ

ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАНА

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Практическая работа 1

по предмету ***«Криптография»***

На тему: «Математические основы криптографии»

Группа: 721-19

Выполнил: **Хакимбеков Дониёрбек**

Принял: Хамидов Шерзод

Ташкент 2021

Scanned by TapScanner

Задание 1

$n > 0$ и $a < 0$ найти $b = a \bmod n$

$b_2 - 102 \bmod 25$

$-102 \bmod 25 = b$

$-102 + 25 \cdot 2 = \underbrace{37}_{n} - 102 \cdot \bmod 25 =$

$= (35)$

Ответ: 35

Задание 2

$(e \cdot d) \cdot \bmod n = 1$

задана e и n найдите d?

($n = 37$ $e = 19$)

$(19\,d) \cdot \bmod \cdot 37 = 1$

$19 \cdot 2 \cdot \bmod \cdot 37 = 1$

отсюда следует $d = 2$

Ответ: $d = 2$

Scanned by TapScanner

Задание 3

$X_2 -> Y_{10}$ $a = 11110000$.

$11110000 = 2^7 \cdot 1 + 2^6 \cdot 1 + 2^5 \cdot 1 + 2^4 + =$

$= 128 + 64 + 32 + 16 = 160 + 80 =$

$160 = 240$ (10)

Задание 4.

$X_8 > Y_{10}$ $a = 2739$

$2739_8 = 2 \cdot 8^3 + 7 \cdot 8^2 + 3 \cdot 8^1 + 9 \cdot 8^1 =$

$= 1024 + 448 + 24 + 72 = 1568$

Задание 5

$X_{16} > Y_{10}$ $1BA$

$A = 10$ $B = 11$

$1BA = 1 \cdot 16^2 + 11 \cdot 16^1 + 10 \cdot 16^0 =$

$= 442.$

Ответ: 442

Scanned by TapScanner