Изучение технических средств защ. инф. в опт. сети

Цель: изучить возможные способы физической и криптографической защиты оптической соединений.

Секретное число стороны A: x - 3

Несекретные числа: D - 8, P - 7

Секретное число стороны Б: X - 2

Несекретные числа: D - 8, P - 7

По алгоритму Диффи-Хеллмана формирования общего шифрования: Задача

1) $Б = D^x \mod P = 8^2 \mod 7 = 64 \mod 7$, 64 = 7·9 + 1, т.е = 1

$A = 8^3 \mod 7 = 512 \mod 7 = 7·73 + 1$, т.е = 1

2) $K = Б^A \mod P = 1^3 \mod 7 = 1 \mod 7 = 7·0,14 + 0,02$, т.е = 0,02

$K = a^Б \mod P = 1^2 \mod 7 = 1 \mod 7 = 7·0,14 + 0,02$, т.е = 0,02