Name Removed

Wireless and Mobile Networking

Homework 10

**P16.2**

p = 23

q = 37

using RSA

n = p\*q = 23\*37 = 851

e needs to be prime with respect to val1 = (p-1)\*(q-1) = 22\*36 = 792

GCD of e & val need to be 1

Possible value of e = 5

e\*d -1 can be divided into val1

5\*d - 1 should be divisible by val1

Possible value of d = 317

Public key = (n, e) = (851, 5)

Private key = (n, d) = (851, 317)

**P16.12**

Message before anything is done (base message in 8x8 grid as question suggests):

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| I |  | A | M |  | D | O | N |
| E |  | W | I | T | H |  | M |
| Y |  | F | I | N | A | L | S |
|  | A | N | D |  | C | A | N |
|  | N | O | W |  | T | A | K |
| E |  | A |  | B | R | E | A |
| K |  | O | R |  | A |  | V |
| A | C | A | T | I | O | N | . |

1. 8-way interleaving before permute

Interleaving step:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| I | E | Y |  |  | E | K | A |
|  |  |  | A | C |  |  | C |
| A | W | F | N | A | A | O | A |
| M | I | I | D | N |  | R | T |
|  | T | N |  |  | B |  | I |
| D | H | A | N | T | R | A | O |
| O |  | L | O | A | E |  | N |
| N | M | S | W | K | A | V | . |

1. 8-way interleaving after permute before transmission

Permute step:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| M | A | O |  | D | N |  | I |
| I | W |  |  | H | M | T | E |
| I | F | L |  | A | S | N | Y |
| D | N | A | A | C | N |  |  |
| W | O | A | N | T | K |  |  |
|  | A | E |  | R | A | B | E |
| R | O |  |  | A | V |  | K |
| T | A | N | C | O | . | I | A |

Interleaving step:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| M | I | I | D | W |  | R | T |
| A | W | F | N | O | A | O | A |
| O |  | L | A | A | E |  | N |
|  |  |  | A | N |  |  | C |
| D | H | A | C | T | R | A | O |
| N | M | S | N | K | A | V | . |
|  | T | N |  |  | B |  | I |
| I | E | Y |  |  | E | K | A |

**P16.23**

Yes, because the cluster heads will have more critical data, so using a more complex security scheme for their communication is good. On the other hand, singular node data is less important by itself, so a less secure scheme that takes less energy is a much better solution for its data transfer.