5

|  |  |
| --- | --- |
|  |  |
| If | | |
|  |  |
|  | | |
|  |  | |  |
| Since both Therefore is the correct encryption of | | |  |

1. The square-and- multiply algorithm has a time complexity of bit operations, from squarings and modular multiplications

With the above procedure, one reduces the size of the squarings and multiplications to and <, before combining. The time complexity becomes O() which can be shorter than assuming

1. The adversary can compare between message m and incorrect decryption x’ to determine which portion corresponds to From there,

Since

He can now determine q and pa from the relation

1. use large capacitors as well in the machine to smooth any power spikes, with diodes to reduce the chance of reverse discharge. In fact, one should use a redundant power supply to prevent the machine from losing power halfway during calculations as well.

Discussed with Sean, Louis, Min Htet, Min Yueq5