BOSTON UNIVERSITY

Jonathan Redwine <jredwine@bu.edu>

Test4: RSA Alice=JR, Bob=MD, Eve=LL

10 messages

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 3:22 PM
To: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>, lucasli@bu.edu, mdim@bu.edu

Begin Test4

Jonathan Redwine <jredwine@bu.edu> Mon, Dec 9, 2019 at 3:36 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: lucasli@bu.edu

N = 929041
e = 195771

On Mon, Dec 9, 2019 at 3:22 PM Michael Dimitriou <mdim@bu.edu> wrote:

> Begin Test4

Jonathan Redwine <jredwine@bu.edu> Mon, Dec 9, 2019 at 3:38 PM
To: jredwine@bu.edu

to myself:
p = 1847
q = 503
phi(N) = 926692
d = 477123
[Quoted text hidden]

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 3:43 PM
To: Jonathan Redwine <jredwine@bu.edu>
Cc: lucasli@bu.edu

e(x)=624658
[Quoted text hidden]

Jonathan Redwine <jredwine@bu.edu> Mon, Dec 9, 2019 at 3:49 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: lucasli@bu.edu

x = 70596
[Quoted text hidden]

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 3:55 PM
To: Jonathan Redwine <jredwine@bu.edu>
Cc: lucasli@bu.edu

Alice confirming Bob decrypted message x=70596
[Quoted text hidden]

BU <lucasli@bu.edu> Mon, Dec 9, 2019 at 4:17 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: Jonathan Redwine <jredwine@bu.edu>

message: 70596

p: 503
q: 1847
[Quoted text hidden]

Jonathan Redwine <jredwine@bu.edu> Mon, Dec 9, 2019 at 4:23 PM
To: BU <lucasli@bu.edu>
Cc: Michael Dimitriou <mdim@bu.edu>

Those p and q values are correct.
[Quoted text hidden]

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 4:26 PM
To: Jonathan Redwine <jredwine@bu.edu>
Cc: BU <lucasli@bu.edu>

message value is correct
[Quoted text hidden]

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 4:27 PM
To: Jonathan Redwine <jredwine@bu.edu>

End Test4
[Quoted text hidden]