



Jonathan Redwine <jredwine@bu.edu>

Test5: RSA Alice=MD, Bob=LL, Eve=JR

8 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 Test5

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 3:25 PM
To: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>, lucasli@bu.edu, mdim@bu.edu

Alice (Mike) sends to Bob (Lucas):
N=35570389
e=4577047

On Mon, Dec 9, 2019 at 3:22 PM Michael Dimitriou <mdim@bu.edu> wrote:
| Begin Test5

BU <lucasli@bu.edu> Mon, Dec 9, 2019 at 4:47 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>

ex 25900457
[Quoted text hidden]

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 4:48 PM
To: BU <lucasli@bu.edu>
Cc: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>

Alice: x=5257160
[Quoted text hidden]

Jonathan Redwine <jredwine@bu.edu> Mon, Dec 9, 2019 at 4:49 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: BU <lucasli@bu.edu>

Eve:
p = 4219
q = 8431
d = 21133363
x = 5257160
[Quoted text hidden]

BU <lucasli@bu.edu> Mon, Dec 9, 2019 at 4:49 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>

x is correct
[Quoted text hidden]

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 4:51 PM
To: Jonathan Redwine <jredwine@bu.edu>
Cc: BU <lucasli@bu.edu>

Alice confirming p and q values are correct. Bob already confirmed x value is correct.

[Quoted text hidden]

Michael Dimitriou <mdim@bu.edu>
To: Jonathan Redwine <jredwine@bu.edu>
Cc: BU <lucasli@bu.edu>

Mon, Dec 9, 2019 at 4:51 PM

End Test5

[Quoted text hidden]