Jonathan Redwine <jredwine@bu.edu>

Test3: ElGamal Alice=LL, Bob=JR, Eve=MD

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 Test3

BU <lucasli@bu.edu> Mon, Dec 9, 2019 at 5:09 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>

g_a = 375881

N = 6238559
g = 2472959

> On Dec 9, 2019, at 3:22 PM, Michael Dimitriou <mdim@bu.edu> wrote:
>
> Begin Test3

Jonathan Redwine <jredwine@bu.edu> Mon, Dec 9, 2019 at 5:09 PM
To: BU <lucasli@bu.edu>
Cc: Michael Dimitriou <mdim@bu.edu>

Bob:
g^b = 5852424
e(x) = 1477344
[Quoted text hidden]

BU <lucasli@bu.edu> Mon, Dec 9, 2019 at 5:10 PM
To: Jonathan Redwine <jredwine@bu.edu>
Cc: Michael Dimitriou <mdim@bu.edu>

x=9393
[Quoted text hidden]

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 5:11 PM
To: BU <lucasli@bu.edu>
Cc: Jonathan Redwine <jredwine@bu.edu>

Eve:
Encrypted message: 9393
Alice's private key a: 5820911
Bobs's private key b: 2185913
[Quoted text hidden]

Jonathan Redwine <jredwine@bu.edu> Mon, Dec 9, 2019 at 5:11 PM

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

The values for x and b are correct.

[Quoted text hidden]

BU <lucasli@bu.edu> Mon, Dec 9, 2019 at 5:12 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: Jonathan Redwine <jredwine@bu.edu>

a is correct

[Quoted text hidden]

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 5:13 PM
To: BU <lucasli@bu.edu>
Cc: Jonathan Redwine <jredwine@bu.edu>

End Test3

[Quoted text hidden]