BOSTON UNIVERSITY

Jonathan Redwine <jredwine@bu.edu>

Test1: ElGamal Alice=JR, Bob=MD, Eve=LL

10 messages

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 3:21 PM
To: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>, Lucasli@bu.edu, mdim@bu.edu

Begin Test1

Jonathan Redwine <jredwine@bu.edu> Mon, Dec 9, 2019 at 3:34 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: Lucasli@bu.edu

Alice:
N = 666527
g = 363887
g^a = 460341

On Mon, Dec 9, 2019 at 3:22 PM Michael Dimitriou <mdim@bu.edu> wrote:
> Begin Test1

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

to myself:
a = 81032
[Quoted text hidden]

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

g^b = 427807
e(x) = 568742
[Quoted text hidden]

Jonathan Redwine <jredwine@bu.edu> Mon, Dec 9, 2019 at 3:50 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: Lucasli@bu.edu

x = 32893
[Quoted text hidden]

Michael Dimitriou <mdim@bu.edu> Mon, Dec 9, 2019 at 3:56 PM
To: Jonathan Redwine <jredwine@bu.edu>
Cc: Lucasli@bu.edu

Alice confirming Bob decrypted message x = 32893
[Quoted text hidden]

BU <lucasli@bu.edu> Mon, Dec 9, 2019 at 4:18 PM
To: Michael Dimitriou <mdim@bu.edu>
Cc: Jonathan Redwine <jredwine@bu.edu>

a: 81032
b: 631439
message: 32893
[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>

That a 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>
Cc: BU <lucasli@bu.edu>

values for b and message are correct
[Quoted text hidden]

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

End Test1
[Quoted text hidden]