



Jonathan Redwine <jredwine@bu.edu>

---

## Test2: ElGamal Alice=MD, Bob=LL, Eve=JR

9 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 Test2

---

**Michael Dimitriou** <mdim@bu.edu> Mon, Dec 9, 2019 at 3:24 PM  
To: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>, lucasli@bu.edu, mdim@bu.edu

Alice (Mike) sends to Bob (Lucas):  
N= 799343  
g= 247704  
g<sup>a</sup>= 63397

On Mon, Dec 9, 2019 at 3:21 PM Michael Dimitriou <mdim@bu.edu> wrote:  
| Begin Test2

---

**BU** <lucasli@bu.edu> Mon, Dec 9, 2019 at 4:27 PM  
To: Michael Dimitriou <mdim@bu.edu>  
Cc: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>

g<sup>b</sup> : 778602  
e(x): 229270  
[Quoted text hidden]

---

**Michael Dimitriou** <mdim@bu.edu> Mon, Dec 9, 2019 at 4:29 PM  
To: BU <lucasli@bu.edu>  
Cc: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>

x = 8743  
[Quoted text hidden]

---

**Jonathan Redwine** <jredwine@bu.edu> Mon, Dec 9, 2019 at 4:31 PM  
To: Michael Dimitriou <mdim@bu.edu>  
Cc: BU <lucasli@bu.edu>

Eve:  
a = 604879  
b = 230155  
x = 8743  
[Quoted text hidden]

---

**Michael Dimitriou** <mdim@bu.edu> Mon, Dec 9, 2019 at 4:32 PM  
To: Jonathan Redwine <jredwine@bu.edu>  
Cc: BU <lucasli@bu.edu>

Alice confirming a = 604879  
[Quoted text hidden]

---

**BU** <lucasli@bu.edu> Mon, Dec 9, 2019 at 4:36 PM  
To: Michael Dimitriou <mdim@bu.edu>

Cc: Jonathan Redwine <jredwine@bu.edu>

Bob confirming b = 230155

[Quoted text hidden]

---

**BU** <lucasli@bu.edu>

Mon, Dec 9, 2019 at 4:37 PM

To: Michael Dimitriou <mdim@bu.edu>

Cc: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>

x=8743

is correct

[Quoted text hidden]

---

**Michael Dimitriou** <mdim@bu.edu>

Mon, Dec 9, 2019 at 4:38 PM

To: BU <lucasli@bu.edu>

Cc: "Redwine, Jonathan, Hewitt" <jredwine@bu.edu>

End Test2

[Quoted text hidden]