Name: Wenliang Sun

1.Solution:

First attack:

Trudy can initiate a connection with Bob saying (“I’m Alice”, R) together. Bob will response E (R, KAB) to Trudy. Then, since Trudy don’t know KAB, she can’t compute E (R+1, KAB), but she can initiate a new connection with Bob by saying, “I’m Alice”, R+1 together. Then, Bob will response E (R+1, KAB). That’s what Trudy needed for previous connection, so using first connection she can send E (R+1, KAB) to Bob. The mutual authentication has been approved by this protocol to Trudy claiming she is Alice. Bob will believe he is talking with Alice.

Second attack:

Trudy can perform replay attack. Trudy gets “E (R+1, KAB)” from Alice and then send it to Bob. Bob will believe she is Alice.

2. Solution:

Alice picks a session key K and sends a signed message containing K which is encrypted by Bob’s public key and a timestamp t. And then Bob responds with the timestamp t encrypted with K.

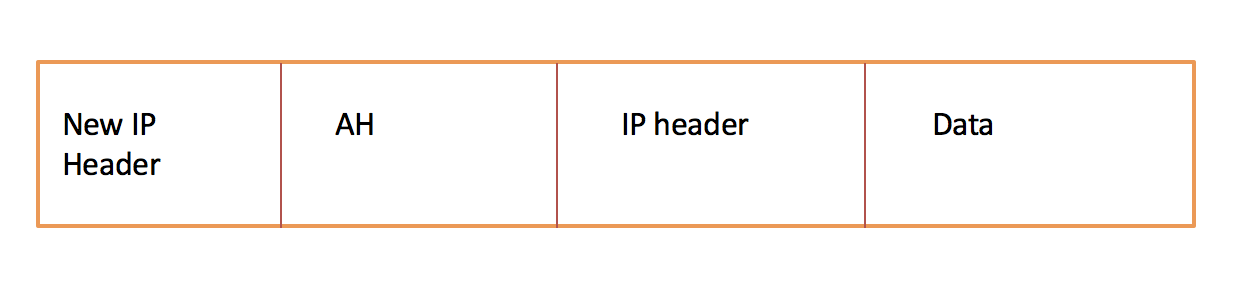
3. Solution:

a) They all have encryption, integrity, authentication functions.

b) IPSec works in IP layer, but SSL works between application layer and transport layer; IPSec is very complex, but SSL is easier; IPSec implementation requires changes to OS, but no changes to applications; SSL implementation requires changes to applications, but no changes to OS; SSL built into Web application early on (Netscape); IPSec used in VPN applications (secure tunnel)

c) For SSL, it uses TCP handshake protocol to establish security context between two parties. For IPSec, it is based on IP protocol.

d) As below:



5.33 Solution:

a) The line’s equation is “y= -2/3x + 6”; S = 6

b) The line’s equation is “5x+6y=9mod13”; S=8

5.42 Solution:

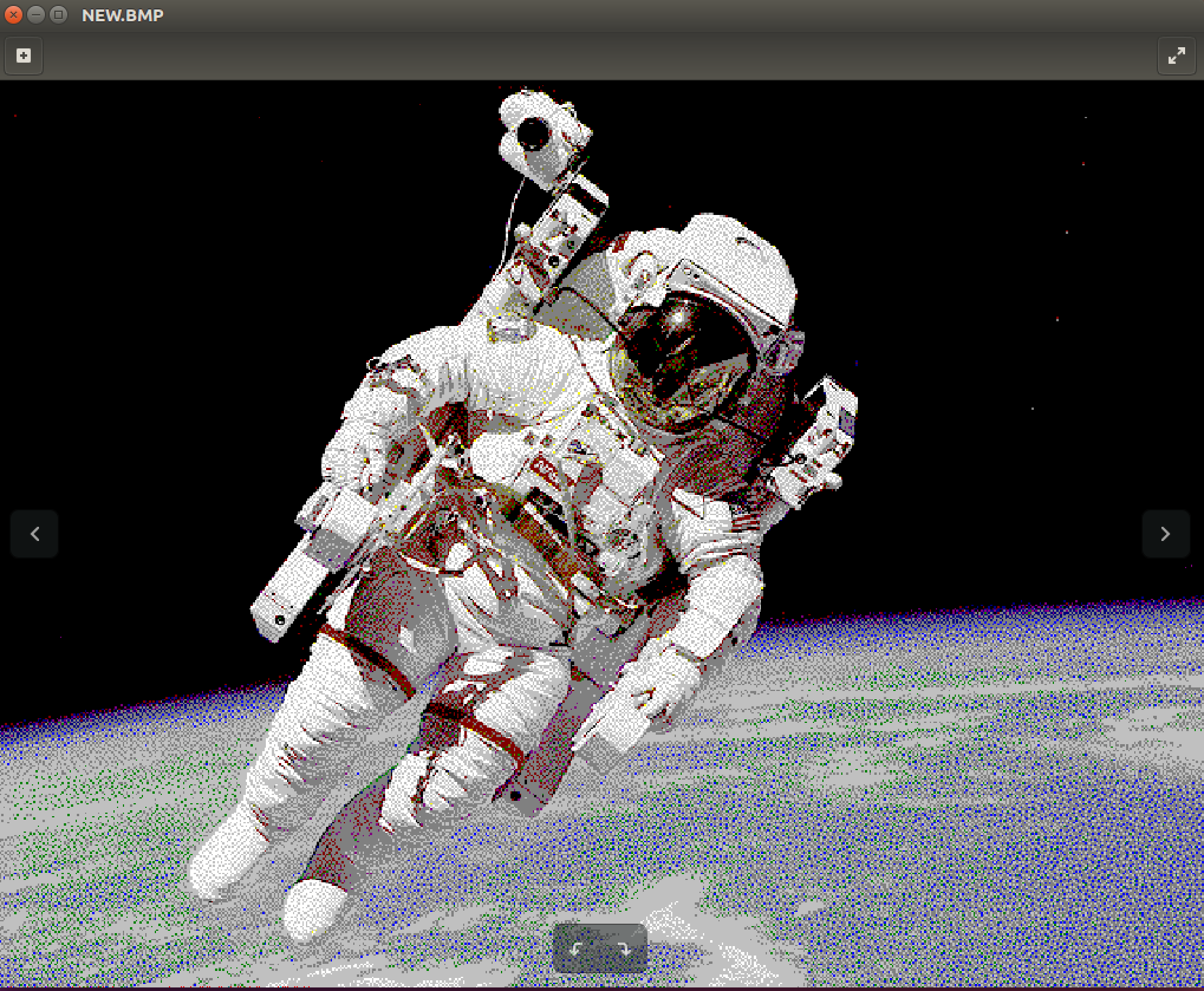
a) A book named “Alice's Adventures in Wonderland”.

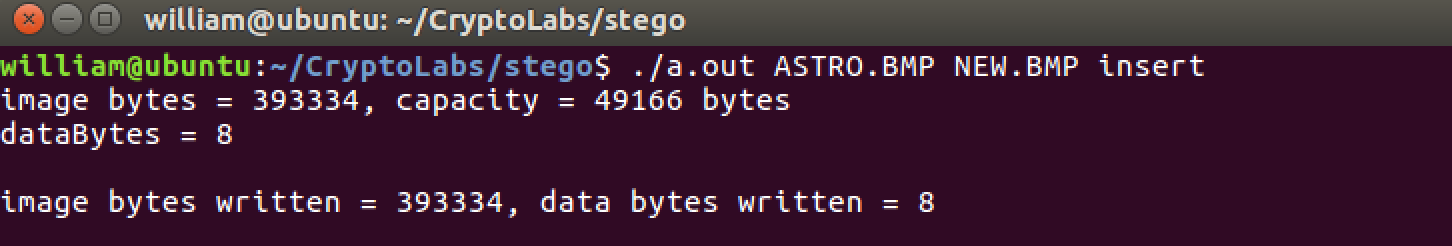
b) and c)

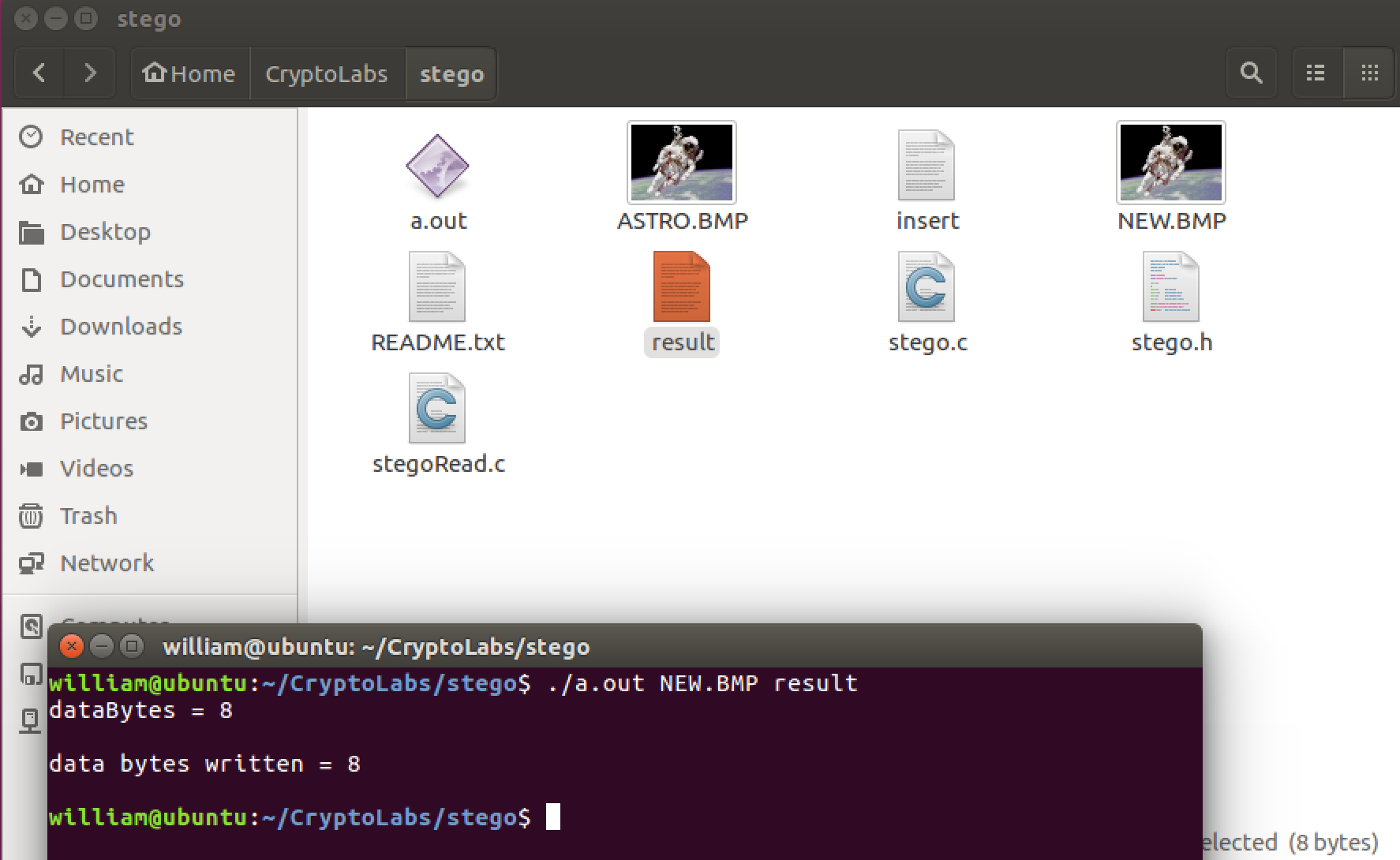
Without hiding info:



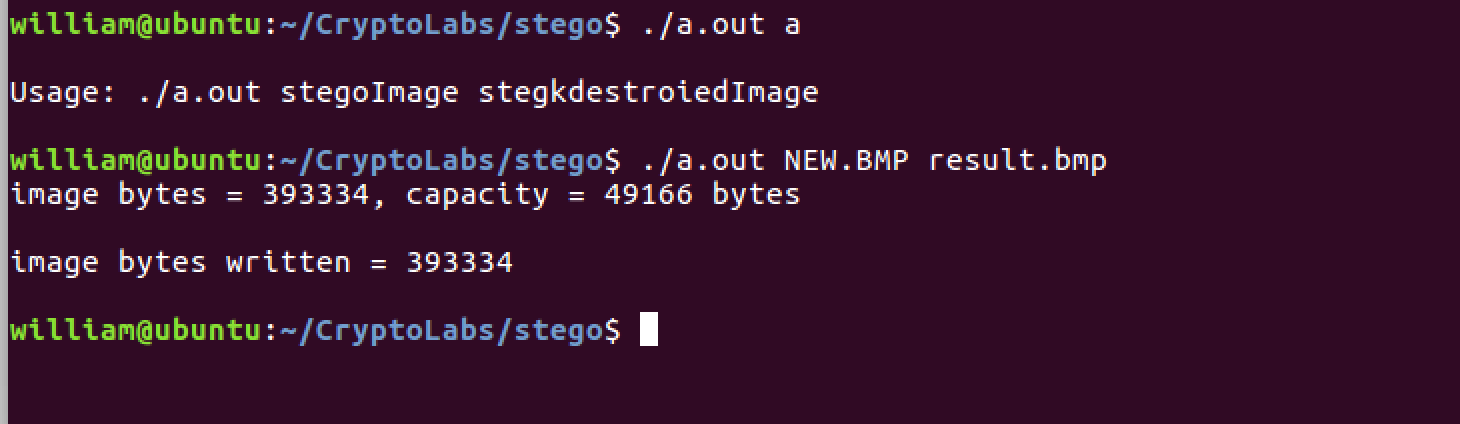
With hiding info:

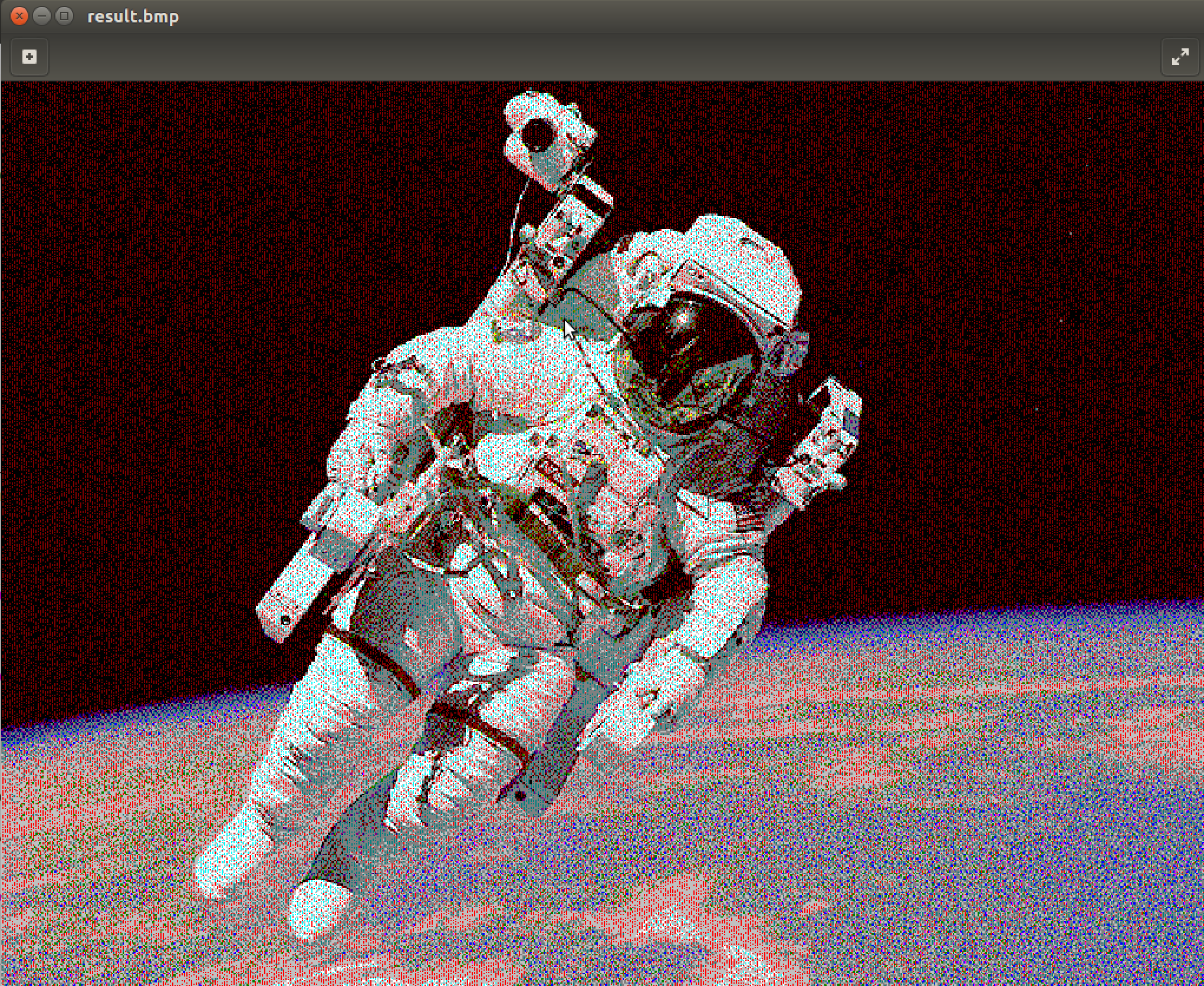


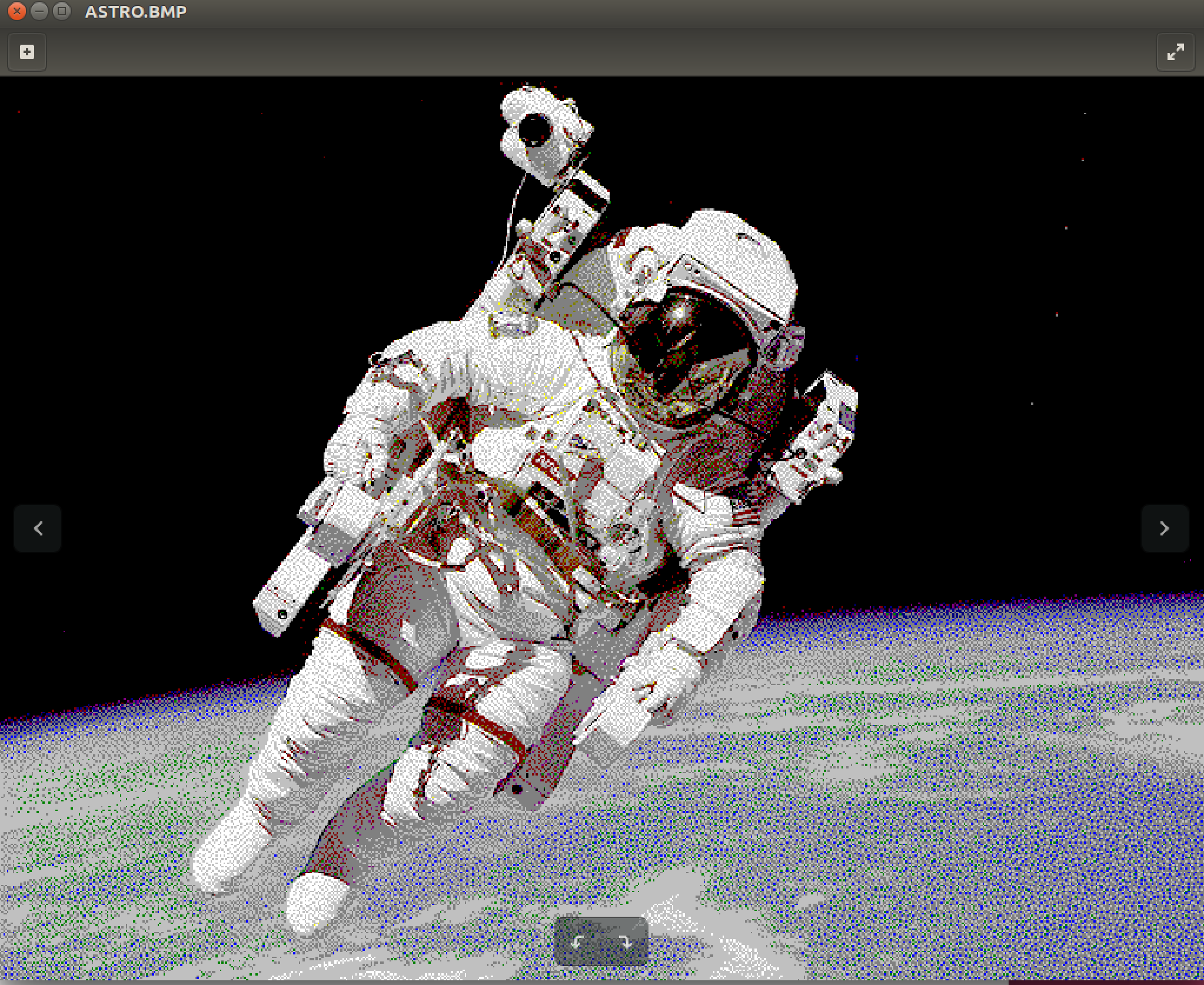


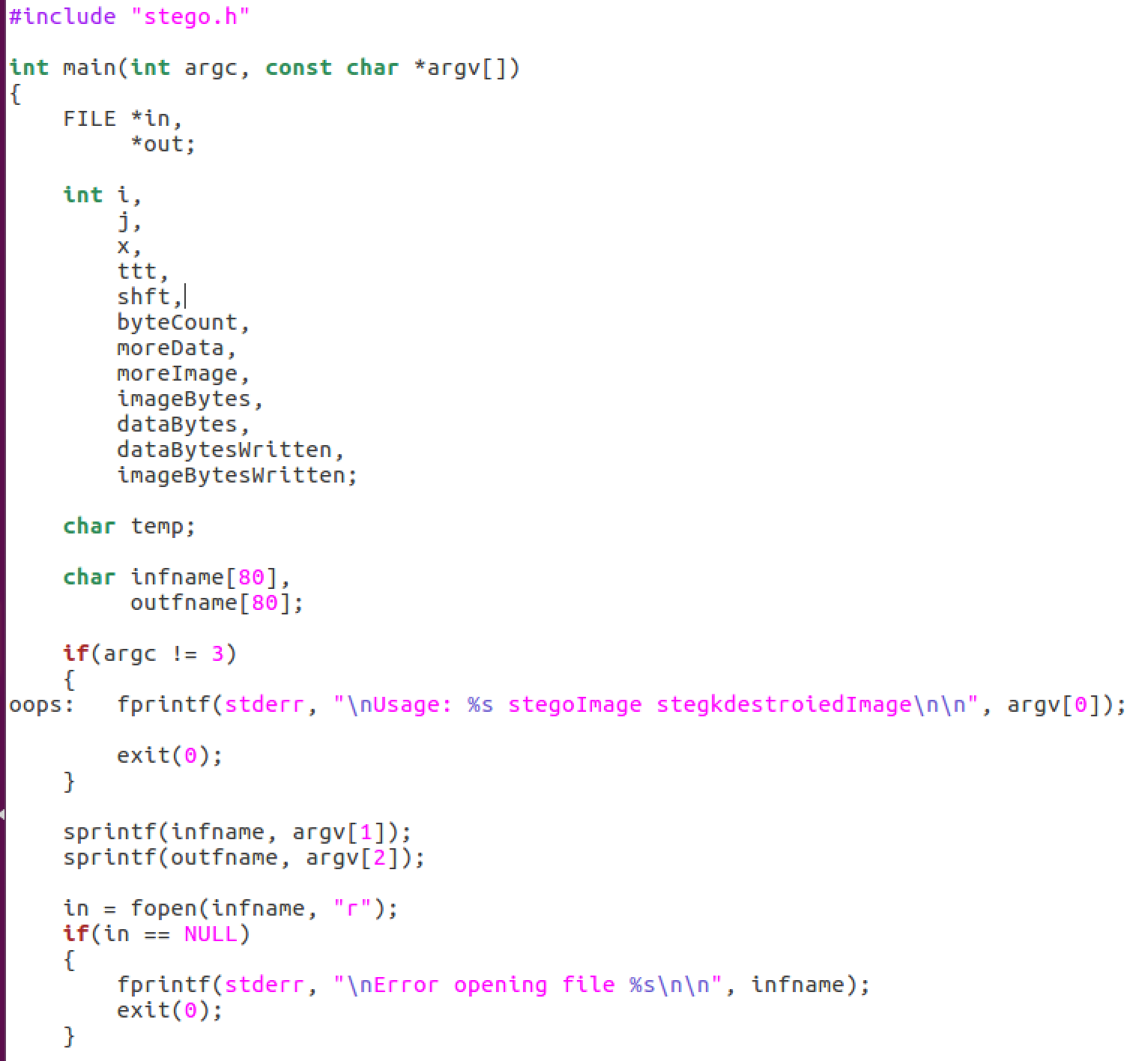
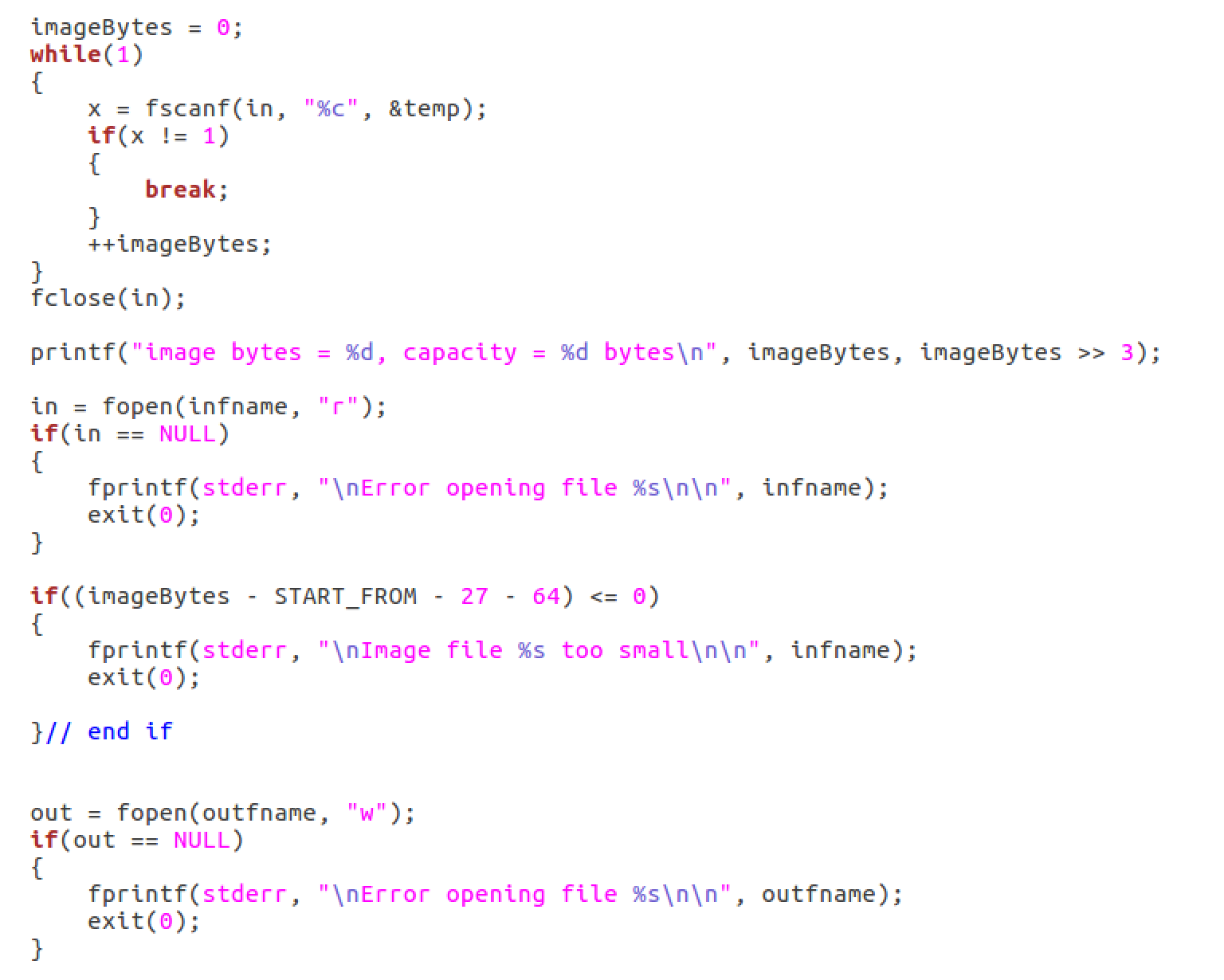


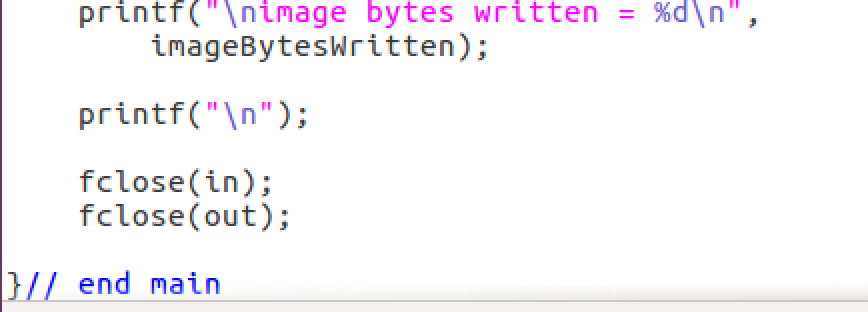
5.43 Solution:



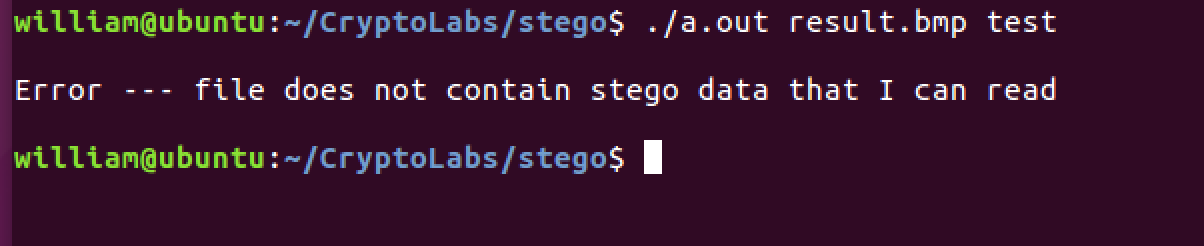




And I cannot extract anything from the result figure.



5.48 Solution:

a) The symmetric keys and IVs.

b) Randomly selecting primes in RSA; randomly generating exponents in DH

5.49 Solution:

a) Because we can predict the next sequence of numbers by the given sequence of numbers. For example, if we use the numbers as a keystream, then a known plaintext attack maybe devastating.

b) Yes, since an attacker might know some plaintext, in which case they would know the keystream bits.

10.1 Solution:

a) The signature SA, since only Alice could have signed it, and Bob can verify the signature. Note that H is included in SA, and H contains Bob’s challenge, RB, so this provides the replay protection.

b) Trudy would have to break the DH key exchange by, presumably, solving an intractable discrete log problem.

c) Put Trudy in the role of Bob. Then after the 4th message, she and Alice will have agreed on a key K=gab mod p. This does not break the protocol-the authentication will fail, since Trudy cannot forge the required signature in message 4. So Alice will terminate the protocol, and she will never use K.

d) In this version of protocol, then encryption serves no purpose. However, in the password version, the encryption does have a purpose.