**CMSC 626 Principles of Computer Security**

**Project**

**Exercise 4**

Faisal Rasheed Khan Shrenik PolySetty

VB02734 AZ61492

[vb02734@umbc.edu](mailto:vb02734@umbc.edu)

1.

1. Team Information:
2. Name: **Faisal Rasheed Khan**

University Id: **VB02734**

1. Name: **Shrenik PolySetty**

University Id: **AZ61492**

1. Prime Number, P = 1065601

Primitive root, α = 7

Xa = 139278

Xb = 111689

Key = 159571

1. nc -l 12345

nc 130.85.220.34 12345

python3 diffehellman.py | nc 130.85.220.34 12345

python3 diffehellman.py <vm1pipe | nc 130.85.220.34 12345 >vm1pipe

nc -l 12345 <vm2pipe | python diffehellman.py >vm2pipe

mkfifo vm1pipe

nc -l 12345 | python3 diffehellman.py

python3 diffehellman.py

cat tcpdumpcapture.cap

nano diffehellman.py

ls

ifconfig -a

tcpdump -D

tcpdump -n -i ens160 -w tcpdumpcapture.cap host 130.85.121.106 and port 12345

tcpdump -n -i ens160 -w tcpdumpcapture.cap host 130.85.220.34 and port 12345

tcpdump -n -i ens160 -w tcpdumpcapture.cap host 130.85.121.106 and port 12345

tcpdump -r capture.pcap

tcpdump -n -i ens160 -w vm1capture2.pcap host 130.85.220.34

1. The challenges faced were:

* While encrypting and decrypting the key, faced issue because key was of int type text

Resolved this issue with the help of converting the int to str ,encoding and decoding with ‘utf-8’

* Faced issue while connecting to the other Virtual Machine to send the encrypted plain text using netcat command

Resolved the issue by passing the command of netcat to subprocess.Popen()

* While encrypting and decrypting the pain text and cipher text, faced issue of unable to decode with ‘utf-8’ as it was in other format

Resolved by removing unnecessary encoding.

* Faced challenges while using wireshark, tshark as access to install that was not there

Resolved using tcpdump command

* The tcpdump command was capturing every data incoming

Resolve by applying proper filters

* For tcpdump command, which interface to use to capture the data was a problem

Resolved by using this command, tcpdump -D

1. Successfully implemented the Diffe-Hellman Key Exchange Algorithm to encrypt and decrypt the text over the communicating channels between two virtual machines while calculating the shared key with their respective private keys, where keys are generated using prime number, primitive root and private key. Learnt different ways of sending the data via command line arguments or incorporating everything in the python file. Successfully implemented the tcpdump/wireshark capture to capture the real time packets sent/received. Can store tcpdump/wireshark capture using .pcap or .cap extension.
2. References:

[CH02-CompSec4e\_accessible\_L03 (blackboardcdn.com)](https://learn-us-east-1-prod-fleet01-xythos.content.blackboardcdn.com/blackboard.learn.xythos.prod/5954eb74c7df4/20853920?X-Blackboard-S3-Bucket=blackboard.learn.xythos.prod&X-Blackboard-Expiration=1676851200000&X-Blackboard-Signature=j2dqL5m2BmuM9DMIXtTGCuDKFGLFvL%2FDBsSyiND3QKM%3D&X-Blackboard-Client-Id=100208&X-Blackboard-S3-Region=us-east-1&response-cache-control=private%2C%20max-age%3D21600&response-content-disposition=inline%3B%20filename%2A%3DUTF-8%27%27CH02-CompSec4e_accessible_L03.pdf&response-content-type=application%2Fpdf&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEP3%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJGMEQCIEQQIAfwL%2B4qxIutoRXaW4vkzvlzQfeM2oh5H21bbDDsAiAC8GDHugloJsm3pz48TRF86QWRfmtCg8OLv9Zqkofw4SrVBAiV%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F8BEAAaDDU1NjkwMzg2MTM2MSIMYejZSnmP5%2BhufHY5KqkETSykdtU%2FtBOXBybTfaE3R2Cj4EjyFPTYHydpIy0jJaiSXHsQvi9XMPEgHr8%2BQgORzgBpWCxGGsd7juTQ8k7ZdPja7treVuK1evvd89jwba%2FXQNKVa1dvCyBUZ6OdYps6vZRVWxbw55G%2B%2BokjnBC2wXiOs3UGgm%2BwiTGtUqAiuQeDIDKLP8Z0zmLXuODBLDMGz91Z6Irv%2B3ABnAsTiEFeTNxHVvfqrBVPycGedW1tV8temBnLKm5nnGsu45NW9WSrSyXq9l7NZQ%2FXL%2Br8XnvZJie0zDAJx4KXe%2FRRvAlSEuUvQwIUYdpfFcdPDb2gK4NuDoAk6kGcAGn8T6XmaJ31zYuFqVX7FfrpOlEmBZHpW88L2wbp1I2SX8xVaMBfktFb2j3dBdUNWHPgqZPH0FY3f%2FyVUg2v05hjXnbfDZRwnKsBfuOeaUI69SCRubJvZWDXFIp%2BmrwOPiCaKD3GgJ3rJ45Pw5dEsft3c%2BDO8IPfq%2Bwwt0MwvdxdE1DFbZex1DlGIJHEd5gMqKIYwV8nzMeNBt4AlAys8NGt1iT%2FS49Ux9fhupE2JvVkH2Edp%2F0pP9XAJo11PZOlneXVcVIMl5FxsGE4rwjFIGAEzghXXNgbu%2BwB2bFz%2BMFB29cvKLlwWnMjyVh17%2Bjd91oC4bx%2Btv4%2FUMSKM9i3ak8Trvw8SifAY83qqBmgSubZsLXKnanvoYYXDCI1QKpkey3E7RRD1xt3NhWPg2HYByy%2B7DDTgcqfBjqqAQE%2B6HLFsyC%2FDsiXA8w8iyoxWQB7GTs8L6BiyY5bTj6GXvlXPSgZmU00zRuLnJBpipWh23oJo51K4G84%2Fua4Sj8hQ7VwNr97hO0uzc%2F5BOFRgkZcWdXaPVfQ0vaVleoL529rwNdxhegvMT4caLqR2G4RhkOL9Kkmbu4xBdcUi08vfSCqIZQrqbBNrCzWOsSBUObXu2qlptJV27dHjax%2FKttseYwEU9UbgANb&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20230219T180000Z&X-Amz-SignedHeaders=host&X-Amz-Expires=21600&X-Amz-Credential=ASIAYDKQORRYTKDDXUVP%2F20230219%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Signature=85d228a59c4b86a35927594bc0046b89cce45cc8be)

[How To Use Netcat to Establish and Test TCP and UDP Connections | DigitalOcean](https://www.digitalocean.com/community/tutorials/how-to-use-netcat-to-establish-and-test-tcp-and-udp-connections)

[L07-CH21-CompSec4e\_accessible (blackboardcdn.com)](https://learn-us-east-1-prod-fleet01-xythos.content.blackboardcdn.com/blackboard.learn.xythos.prod/5954eb74c7df4/21143920?X-Blackboard-S3-Bucket=blackboard.learn.xythos.prod&X-Blackboard-Expiration=1678093200000&X-Blackboard-Signature=DW6cy%2F8kGRywyR4Uz1aTD4LE0GlqRY%2BGXV%2ByhXk90PI%3D&X-Blackboard-Client-Id=100208&X-Blackboard-S3-Region=us-east-1&response-cache-control=private%2C%20max-age%3D21600&response-content-disposition=inline%3B%20filename%2A%3DUTF-8%27%27L07-CH21-CompSec4e_accessible.pdf&response-content-type=application%2Fpdf&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEFUaCXVzLWVhc3QtMSJHMEUCICtOHmLIPqUPU6iwUCKXjzDvtSxgDiV2xUashAA2PfioAiEAnFjnrbRJxZhsBSMk2VU6amhzrfGGpa5hlYbyrbdY5joquwUI%2Fv%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FARAAGgw1NTY5MDM4NjEzNjEiDBhfBAZQKdP0I%2FSlGSqPBZk9cCUrcoqcPv8e0Zzf8cEkOn4Jlye6gIPDBR2bR9KTt7dxCMwpS77vX5uZBu5GB8NUlpL8xppxCgBFVMt2feokJgqlqTBhtjaIEopVV167ZS1Ie8CV%2B2O4CuHyT%2FyLFxrGl0O%2Fqyb5ShsSquUScrWBGqGxbAXFvzg8wVx%2FS3o94fxlE%2FYcACn7IxfHaL2dF8Zd9K7dh%2BSG6G7iZ%2FVezsqEKSUpbP2LdxtGSlhItblHX58l7twvXLbvaH6mpZl1HtvknGo7u2ascB9BE7gCR5PWHpcuKurh2TkkOYIZsjEbRnM2hnq%2FlKjKS5C04cPHlEpd%2BenONZBuIftPLOHtv%2BdxnIsfymP%2BdAg674n1wpoMHXiyMm1M%2BpyTQjhZ78N0yY9x7GM7rCx8HFGFMiRm2hjyhxH7hNjpPNZN%2BuxSLeGQPf9HEv87iEVAzbHIrfeLRcxZs8KcHdx9nHhR54dbC3hVNExW9vG2f9kiAOdTx6EJnV2y1wslTSRX9OO2CaA6Zlp0lZ73QIFjpT0LGQL5Q4xtrNZqFB4ZfP4lLQfUw66Y30FknImiqAyi45nZzyjtjqZYWdDg6MveBNfDPVTeumpnFdgvsEJNBZ3rhZJLlpBFyK2qakNnRVEDL5vuKmq3IhnJvP7bO7u56%2Bdy8%2FDFK50umZGJMA8fSG%2BI14eS3u1JKzA6W87nUudtJxQ5sMt4N2AsucfzElAK5nz86pkqZxdaj3i4vMkOOvUw%2FWEf%2F7atvbimtRrCYu2lCRwlHhW%2BV%2FhRqblooDSKIAF7aEOCr%2BuXeX%2F3lMeXKx%2BVae3FIP29KalC2LuhiGGxiPgJnfwyV8efg1mhU3zZYuici2jKcRjlHy4vAk%2BpEh67rlIpLQkwmt%2BVoAY6sQH3enpFBbb6hQmSi%2BiBZNhaGMmamKs2eKfa8RYwGlGwUpC3OZCDesZkvtG0a%2BsazJvn9nRf%2BaWFNOvF%2Fs9oXDYOCb%2FTefMSydEd7q%2FGU0Bb96LvcglO3A5Qs812%2Fksy7VHliGFSjvKaOy0x3l3%2BFzC52637EGmayEJoW%2FpaR2gXOPwaOSXvG183vsOG%2BloR%2FArMxL4OAc0agtb74J48Hk1xIWGcGH%2F4lNvEnuluAQQFZh8%3D&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20230306T030000Z&X-Amz-SignedHeaders=host&X-Amz-Expires=216)

[Primitive Root - Algorithms for Competitive Programming (cp-algorithms.com)](https://cp-algorithms.com/algebra/primitive-root.html)

[tcp\_client.py](file:///C:\Users\juver\Downloads\tcp_client.py)

[tcp\_server.py](file:///C:\Users\juver\Downloads\tcp_server.py)

[RC4-KeyGeneration(1).py](file:///C:\Users\juver\Downloads\RC4-KeyGeneration(1).py)

[subprocess — Subprocess management — Python 3.11.2 documentation](https://docs.python.org/3/library/subprocess.html)

[Tcpdump Command in Linux | Linuxize](https://linuxize.com/post/tcpdump-command-in-linux/)

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text

Description automatically generated