ДОДАТОК А

Програма на мові Python для розшифровки ключа в повідомленні Plugguble Transport obfs2

```
>>> from Crypto.Cipher import AES
>>> from Crypto.Util import Counter
>>> from hashlib import sha256
>>> seed = «1cf11191affb8f3108c7a653c38410a1».decode(«hex»)
>>> secret = sha256(«Initiator obfuscation padding» + seed + «Initiator obfuscation padding»).digest()
>>> key = secret[0:16]
>>> ctr = secret[16:32]
>>> aes = AES.new(key, AES.MODE_CTR, counter=Counter.new(128, initial_value=long(ctr.encode(«hex»), 16)))>>> ciphertext = «e5d1ecbb726840272562bb8bc25b571a».decode(«hex»)
>>> print(aes.decrypt(ciphertext).encode(«hex»))
e5d1ecbb726840272562bb8bc25b571a
```

ДОДАТОК Б

Програма на мові Python для впровадження механізму Port Knocking

```
from http.server import HTTPServer, BaseHTTPRequestHandler
import os

class MySimpleHTTPRequestHandler(BaseHTTPRequestHandler):
'''Request handler based on BaseHTTPRequestHandler class'''

    services = ['vpn']

    def do_GET(self):
        service = self.requestline.split('/')[2]
        switch = self.requestline.split('/')[3]

        if service in self.services:
            remote_ip = self.headers.items()[0][1]
            if switch == 'on':
                self.send_response(200)
                self.end_headers()
                os.system(f'sudo iptables -t nat -I PREROUTING -s {remote_ip} \
                        -p tcp --dport 443 -j REDIRECT --to-ports 1080')
                self.wfile.write(b'The rule is added. ')
            elif switch == 'off':
                self.send_response(200)
                self.end_headers()
                os.system(f'sudo iptables -t nat -D PREROUTING -s {remote_ip} \
                        -p tcp --dport 443 -j REDIRECT --to-ports 1080')
                self.wfile.write('The rule was deleted.'.encode())
            else:
                self.send_response(400)
                self.end_headers()
                self.wfile.write(f'Unfamiliar switch. Use only: on or off'.encode())
        else:
```

```
            self.wfile.write(‘Unfamiliar service.’)

httpd = HTTPServer(('localhost', 8080), MySimpleHTTPRequestHandler)
httpd.serve_forever()
```

ДОДАТОК В

Повна конфігурація серверу Nginx для налаштування фронтингу доменів із використанням Port Knocking та програми wstunnel

```
events {
      }
http {
  server {
   listen 443 ssl;
   server_name mydomain.net;
   ssl_certificate /etc/nginx/issued/server.crt;
   ssl_certificate_key /etc/nginx/private/server.key;

   location / {
    root /www/data;
    index index.html
    }
   location ~ ^/secret/vpn/on {
    auth_basic      ‘Administrator Login’;
    auth_basic_user_file  /var/www/.htpasswd;
    proxy_set_header X-Real-IP     $remote_addr;
    proxy_pass http://127.0.0.1:8080;
    }
   location /secret2/ws {
    proxy_pass http://127.0.0.1:8090;
    proxy_http_version        1.1;
    proxy_set_header Upgrade 'websocket';
    proxy_set_header Connection 'upgrade';
    proxy_set_header Host 'mydomain.net';
    proxy_set_header X-Real-IP $remote_addr;
    }

  }
}
```

ДОДАТОК Г

Зміна пропускної здатності каналу при прямому підключенні через порт 1194

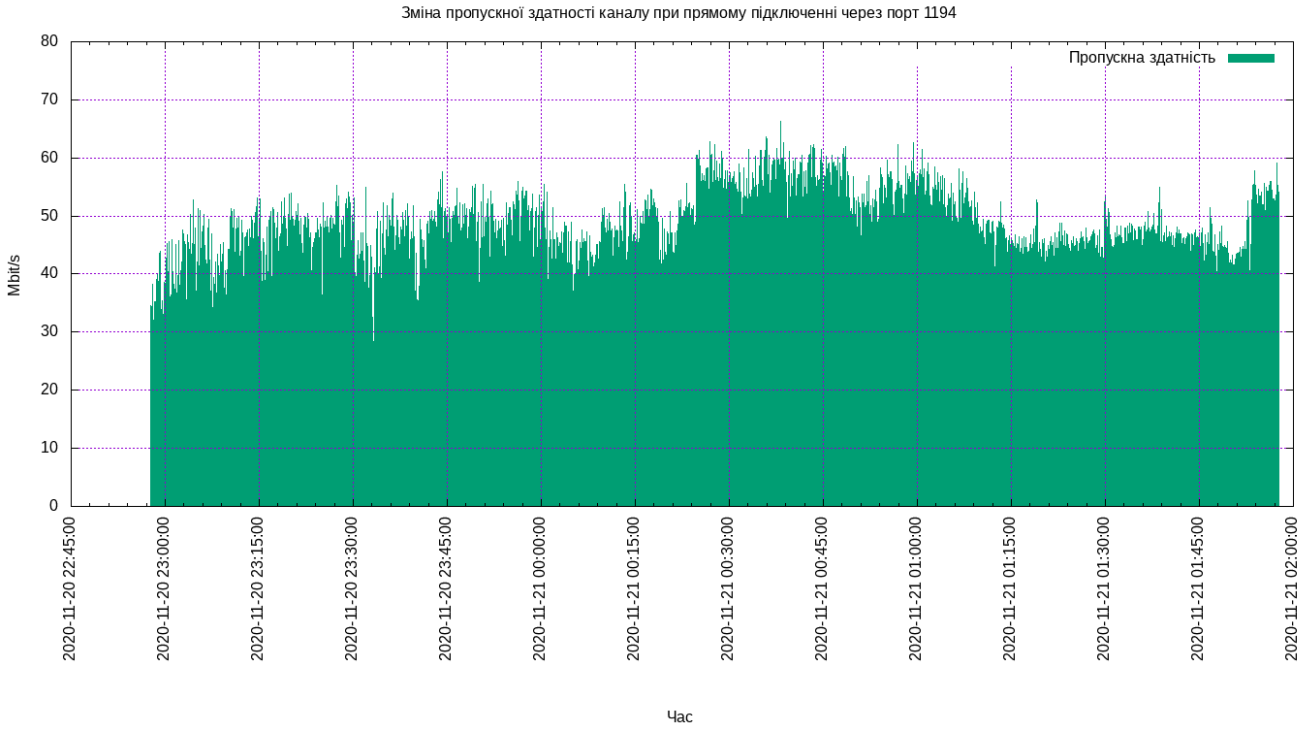

Рисунок Г.1 – Зміна пропускної здатності каналу при прямому підключенні через порт 1194