

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



Môn: Thực tập cơ sở

BÀI BÁO THỰC TẬP CƠ SỞ

Bài 15: Lập trình client/server để trao đổi thông tin an toàn

Họ và tên giảng viên:	TS.Đinh Trường Duy
Họ và tên:	Nguyễn Quốc Khánh
Mã sinh viên:	B20DCAT103
Lớp:	D20CQAT03-B
Số điện thoại:	0964137761

Hà Nội 2023

I. Nội dung lý thuyết:

- Socket là một điểm cuối của liên kết giao tiếp hai chiều giữa hai chương trình chạy trên mạng. Nghĩa là một socket được sử dụng để cho phép 1 chương trình giao tiếp với 1 chương trình khác.

- Các lớp Socket được sử dụng để tiến hành kết nối giữa client và server. Nó được ràng buộc với một cổng port (thể hiện là một con số cụ thể) để các tầng TCP (TCP Layer) có thể định danh ứng dụng mà dữ liệu sẽ được gửi tới.

- Các lớp Socket được sử dụng để tiến hành kết nối giữa client và server. Nó được ràng buộc với một cổng port (thể hiện là một con số cụ thể) để các tầng TCP (TCP Layer) có thể định danh ứng dụng mà dữ liệu sẽ được gửi tới.

- Một đầu của kết nối ngang hàng của ứng dụng mạng phân tán dựa trên TCP/IP được mô tả bởi ổ cắm được xác định bởi:

- Địa chỉ Internet
- Giao thức giao tiếp: UDP, TCP
- Số cổng(Port)

- Các ứng dụng Socket thường là các ứng dụng C hoặc C ++ bằng cách sử dụng Socket API. Một số ngôn ngữ khác như Java, Python cũng cung cấp Socket API. Các ứng dụng Client/Server dựa trên Java, Python khai thác các dịch vụ Socket đó.

II. Nội dung thực hành:

1. Lập trình client và server với TCP socket:

- Mã nguồn của server và chạy thành công server:

```
from socket import *
from hashlib import *
server_name = '127.0.0.1'
server_port = 12080
salt = 'B20DCAT103'
server_socket = socket(AF_INET, SOCK_STREAM)
server_socket.bind((server_name, server_port))
server_socket.listen(1)
print("Server san sang de hoạt động")
while True:
    connect_socket, addr = server_socket.accept()
    string = connect_socket.recv(1024).decode('utf-8')

    message = "Xin chào, đây là server của B20DCAT103"

    connect_socket.send(message.encode())
    connect_socket.close()
```

Command Prompt - d

Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khanh>echo Nguyen Quoc Khanh B20DCAT103
Nguyen Quoc Khanh B20DCAT103

C:\Users\khanh>date
The current date is: Fri 05/12/2023
Enter the new date: (mm-dd-yy)

- Mã nguồn của client và chạy thành công client:

```
from socket import *
from hashlib import *
server_name = '127.0.0.1'
server_port = 12080
salt = 'B20DCAT1033'
client_socket = socket(AF_INET, SOCK_STREAM)
client_socket.connect((server_name, server_port))
string = 'Xin chao, day la client cua B20DCAT171 '
print('Dang gui tin nhan:', string)
client_socket.send(string.encode('utf-8'))
client_message = client_socket.recv(1024)
print("Thong bao tu Server:", client_message.decode('utf-8'))
client_socket.close()
```

```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khanh>echo Nguyen Quoc Khanh B20DCA
T103
Nguyen Quoc Khanh B20DCAT103

C:\Users\khanh>date
The current date is: Fri 05/12/2023
Enter the new date: (mm-dd-yy)
```

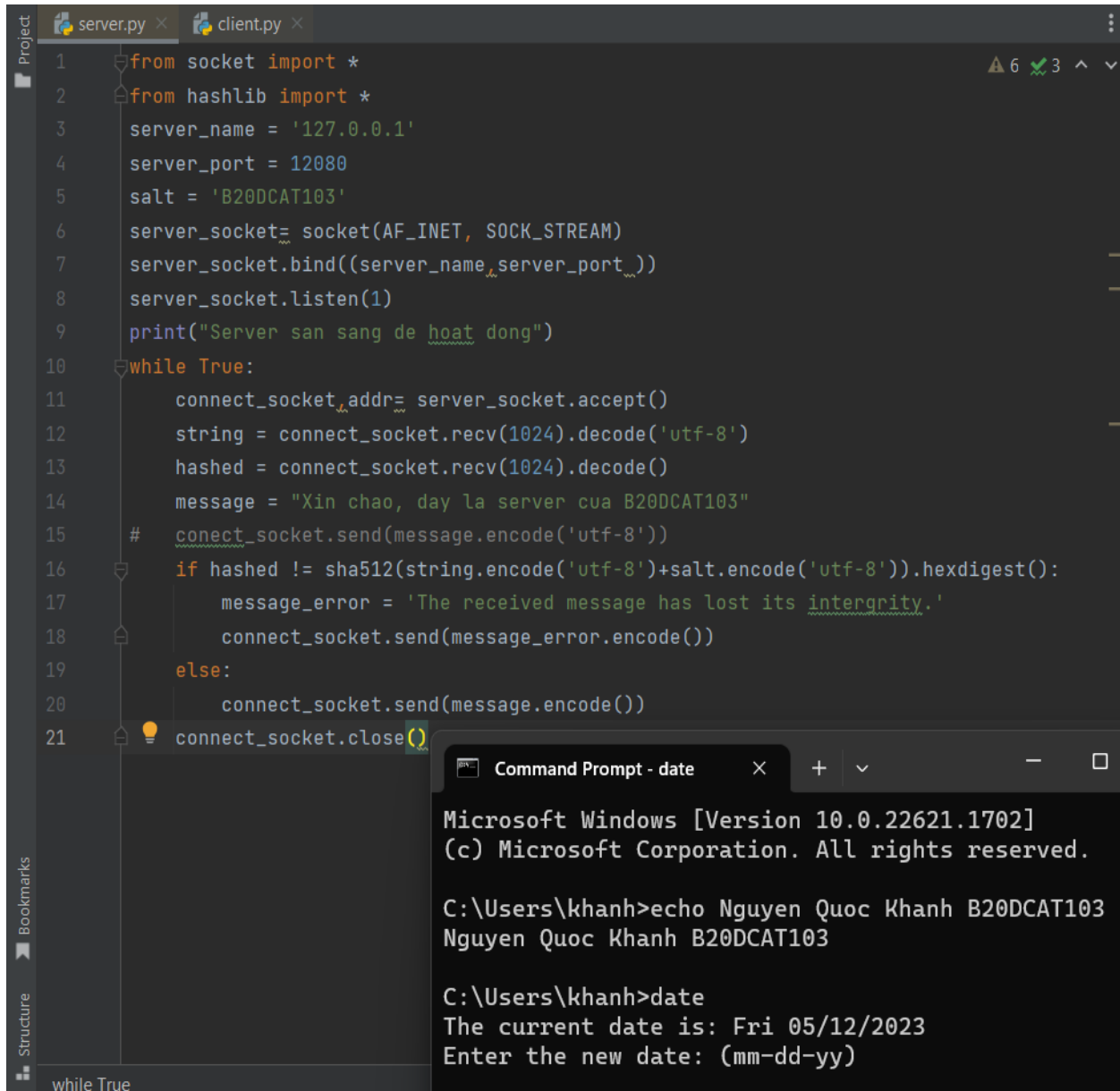
- Bắt gói tin chương trình gửi đi bằng Wireshark:

The image shows two windows side-by-side. The left window is Wireshark, titled '*Adapter for loopback traffic capture'. It displays a list of captured packets in the 'Packet List' pane. The selected packet is number 33, which is an Internet Protocol Version 4 packet from 127.0.0.1 to 127.0.0.1. The 'Packet Details' pane shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, and a data payload. The 'Packet Bytes' pane shows the raw hex and ASCII data of the packet, which includes the string 'Xin chao, day la client cua B20DCAT171'.

The right window is a Command Prompt titled 'Command Prompt - d'. It shows the execution of the client program. The user enters the command 'echo Nguyen Quoc Khanh B20DCA T103' and the output is 'Nguyen Quoc Khanh B20DCAT103'. Then, the user enters the command 'date' and the output is 'The current date is: Fri 05/12/2023'. The prompt then asks 'Enter the new date: (mm-dd-yy)'.

2. Trao đổi thông điệp giữa client và server và đảm bảo tính toàn vẹn của thông điệp khi trao đổi

- Mã nguồn của server và chạy thành công server:



The image shows a code editor with two tabs: `server.py` and `client.py`. The `server.py` tab is active, displaying the following Python code:

```
1 from socket import *
2 from hashlib import *
3 server_name = '127.0.0.1'
4 server_port = 12080
5 salt = 'B20DCAT103'
6 server_socket = socket(AF_INET, SOCK_STREAM)
7 server_socket.bind((server_name, server_port))
8 server_socket.listen(1)
9 print("Server san sang de hoạt động")
10 while True:
11     connect_socket, addr = server_socket.accept()
12     string = connect_socket.recv(1024).decode('utf-8')
13     hashed = connect_socket.recv(1024).decode()
14     message = "Xin chào, đây là server của B20DCAT103"
15     # connect_socket.send(message.encode('utf-8'))
16     if hashed != sha512(string.encode('utf-8') + salt.encode('utf-8')).hexdigest():
17         message_error = 'The received message has lost its integrity.'
18         connect_socket.send(message_error.encode())
19     else:
20         connect_socket.send(message.encode())
21     connect_socket.close()
```

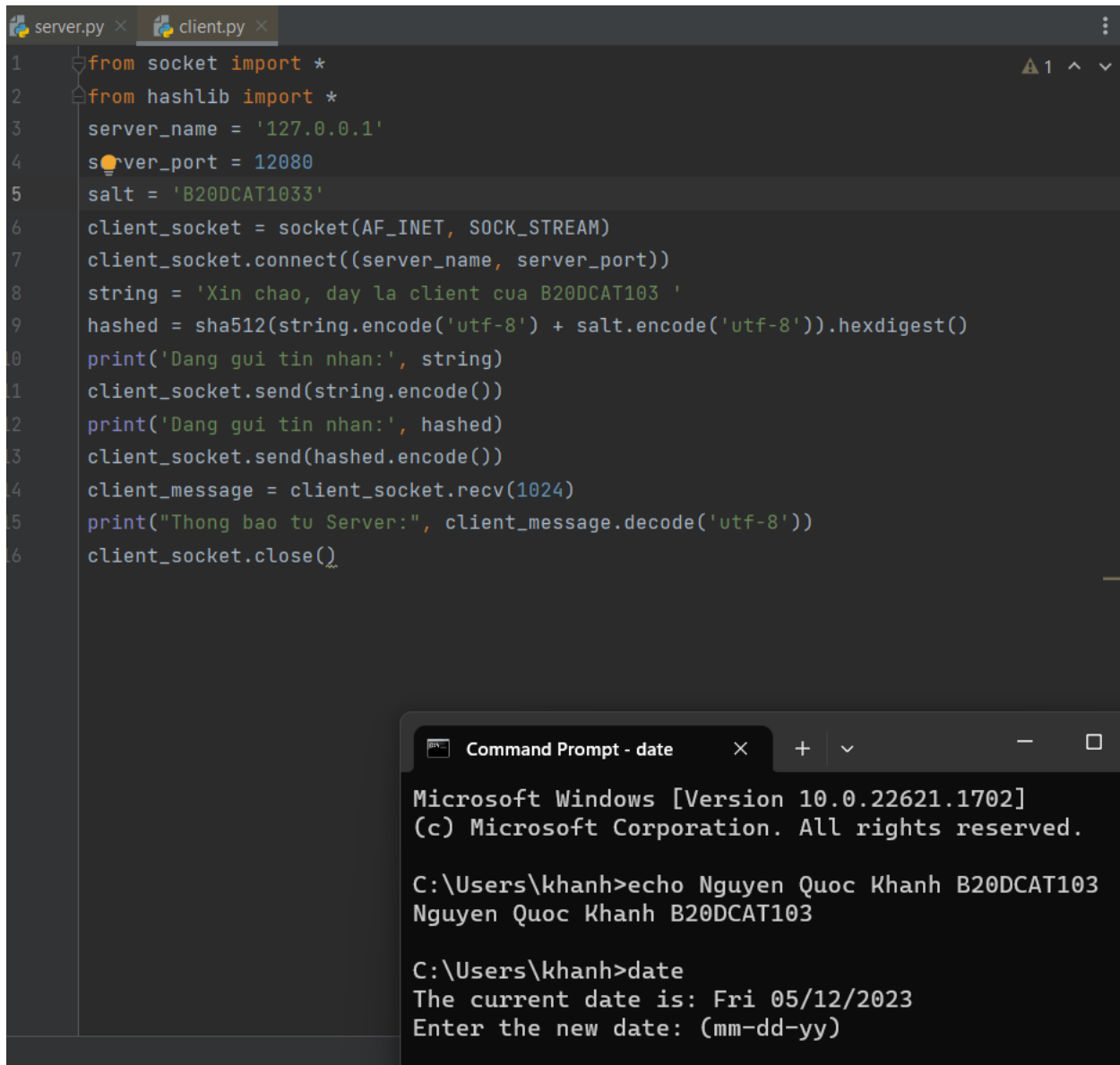
Below the code editor, a Windows Command Prompt window is open, showing the following commands and output:

```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khanh>echo Nguyen Quoc Khanh B20DCAT103
Nguyen Quoc Khanh B20DCAT103

C:\Users\khanh>date
The current date is: Fri 05/12/2023
Enter the new date: (mm-dd-yy)
```

- Mã nguồn của client và chạy thành công client:



The image shows a code editor with two tabs: 'server.py' and 'client.py'. The 'client.py' tab is active, displaying the following Python code:

```
1 from socket import *
2 from hashlib import *
3 server_name = '127.0.0.1'
4 server_port = 12080
5 salt = 'B20DCAT1033'
6 client_socket = socket(AF_INET, SOCK_STREAM)
7 client_socket.connect((server_name, server_port))
8 string = 'Xin chao, day la client cua B20DCAT103 '
9 hashed = sha512(string.encode('utf-8') + salt.encode('utf-8')).hexdigest()
10 print('Dang gui tin nhan:', string)
11 client_socket.send(string.encode())
12 print('Dang gui tin nhan:', hashed)
13 client_socket.send(hashed.encode())
14 client_message = client_socket.recv(1024)
15 print("Thong bao tu Server:", client_message.decode('utf-8'))
16 client_socket.close()
```

Below the code editor, a Windows Command Prompt window is open, titled 'Command Prompt - date'. It displays the following text:

```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khanh>echo Nguyen Quoc Khanh B20DCAT103
Nguyen Quoc Khanh B20DCAT103

C:\Users\khanh>date
The current date is: Fri 05/12/2023
Enter the new date: (mm-dd-yy)
```

- Thay đổi key của client, chạy lại client, và nhận được thông báo “The received message has lost its integrity.”:

```

from socket import *
from hashlib import *
server_name = '127.0.0.1'
server_port = 12080
salt = 'B20DCAT1033'
client_socket = socket(AF_INET, SOCK_STREAM)
client_socket.connect((server_name, server_port))
string = 'Xin chao, day la client cua B20DCAT103 '
hashed = sha512(string.encode('utf-8') + salt.encode('utf-8')).hexdigest()
print('Dang gui tin nhan:', string)
client_socket.send(string.encode())
print('Dang gui tin nhan:', hashed)
client_socket.send(hashed.encode())
client_message = client_socket.recv(1024)
print("Thong bao tu Server:", client_message.decode('utf-8'))
client_socket.close()

```

```

Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khanh>echo Nguyen Quoc Khanh B20DCAT103
Nguyen Quoc Khanh B20DCAT103

C:\Users\khanh>date
The current date is: Fri 05/12/2023
Enter the new date: (mm-dd-yy)

```

```

C:\Users\khanh\PycharmProjects\pythonProjectAI\venv\Scripts\python.exe C:\Users\khanh\PycharmProjects\pythonProjectAI\venv\Scripts\python.exe C:\Users\khanh\PycharmProjects\pythonProjectAI\venv\Scripts\python.exe
Dang gui tin nhan: Xin chao, day la client cua B20DCAT103
Dang gui tin nhan: c1a5f37de04d6fc12beee7353e23597e4aa25c7c29ee1ebe3810d9586136ef
Thong bao tu Server: The received message has lost its integrity.

Process finished with exit code 0

```

- Bắt các gói tin bằng Wireshark: Gói tin thông báo “The received message has lost its integrity.” từ server:

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-F>
No. Time Source Destination Protocol Length Info
33 1.005710 127.0.0.1 127.0.0.1 TCP 89 12080 -> 55820 [PSH, A
34 1.005759 127.0.0.1 127.0.0.1 TCP 44 55820 -> 12080 [ACK] S
35 1.005778 127.0.0.1 127.0.0.1 TCP 44 12080 -> 55820 [FIN, A
36 1.005785 127.0.0.1 127.0.0.1 TCP 44 55820 -> 12080 [ACK] S
37 1.005799 127.0.0.1 127.0.0.1 TCP 44 55820 -> 12080 [FIN, A
38 1.005822 127.0.0.1 127.0.0.1 TCP 44 12080 -> 55820 [ACK] S
39 1.043247 127.0.0.1 127.0.0.1 TLSv1.2 238 Application Data
40 1.043247 127.0.0.1 127.0.0.1 TLSv1.2 238 Application Data
41 1.043261 127.0.0.1 127.0.0.1 TLSv1.2 238 Application Data
42 1.043293 127.0.0.1 127.0.0.1 TCP 44 57773 -> 49696 [ACK] S
43 1.043304 127.0.0.1 127.0.0.1 TCP 44 49696 -> 57773 [ACK] S

> Frame 33: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{...}
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

0000 02 00 00 00 45 00 00 55 bb 1b 40 00 80 06 00 00 ....E..U..@....
0010 7f 00 00 01 7f 00 00 01 2f 30 da 0c 64 ad c9 64 ...../0..d...
0020 30 91 5c e0 50 18 20 fa 45 7e 00 00 54 68 65 20 0.\P...E...The
0030 72 65 63 65 69 76 65 64 20 6d 65 73 73 61 67 65 received message
0040 20 68 61 73 20 6c 6f 73 74 20 69 74 73 20 69 6e has lost its in
0050 74 65 72 67 72 69 74 79 2e tergrity.

Packets: 70 · Disallowed: 0 (0.0%) · Dropped: 0 (0.0%) · Profile: Default

```

```

Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khanh>echo Nguyen Quoc Khanh B20DCAT103
Nguyen Quoc Khanh B20DCAT103

C:\Users\khanh>date
The current date is: Fri 05/12/2023
Enter the new date: (mm-dd-yy)

```

- Gói tin chứa mã hash từ client:

The image shows a network capture in Wireshark and a Windows Command Prompt window. The Wireshark window displays a list of network packets, with the selected packet (No. 27) expanded to show its details. The packet is an Internet Protocol Version 4 (IPv4) packet from 127.0.0.1 to 127.0.0.1. The details pane shows the packet structure, including the Ethernet II header, Internet Protocol Version 4 header, and the payload. The payload is a 172-byte message, which is a Base64-encoded hash. The Command Prompt window shows the execution of the 'echo' command, displaying the output: 'Nguyen Quoc Khanh B20DCA T103'.

Wireshark Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
12	0.307170	127.0.0.1	127.0.0.1	TCP	56	32682 → 55663 [SYN, #
13	0.307194	127.0.0.1	127.0.0.1	TCP	44	55663 → 32682 [ACK] S
14	0.307230	127.0.0.1	127.0.0.1	TCP	57	55663 → 32682 [PSH, A
15	0.307241	127.0.0.1	127.0.0.1	TCP	44	32682 → 55663 [ACK] S
16	0.457931	127.0.0.1	127.0.0.1	TCP	693	32682 → 55663 [PSH, A
17	0.457957	127.0.0.1	127.0.0.1	TCP	44	55663 → 32682 [ACK] S
18	0.458024	127.0.0.1	127.0.0.1	TCP	44	32682 → 55663 [FIN, #
19	0.458036	127.0.0.1	127.0.0.1	TCP	44	55663 → 32682 [ACK] S
20	0.477488	127.0.0.1	127.0.0.1	TCP	44	55663 → 32682 [FIN, #
21	0.477507	127.0.0.1	127.0.0.1	TCP	44	32682 → 55663 [ACK] S

Wireshark Packet Details (Frame 27):

- Frame 27: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface \Device\NPF_{...}
- Null/Loopback
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Wireshark Packet Payload (Hex):

```

0000  02 00 00 00 45 00 00 a8 b2 df 40 00 80 06 00 00  ....E..@....
0010  7f 00 00 01 7f 00 00 01 d9 71 2f 30 1a 13 48 3e  .....q/0..H>
0020  b6 98 07 54 50 18 20 fa 38 11 00 00 37 34 38 30  ...TP...8...7480
0030  66 63 37 39 30 62 35 32 31 38 30 34 37 64 34 65  fc790b52 18047d4e
0040  36 31 66 33 37 31 34 39 61 32 62 66 66 37 66 66  61f37149 a2bfff7f
0050  62 31 39 66 32 62 35 39 32 63 37 65 63 66 61 32  b19f2b59 2c7ecfa2
0060  32 35 64 64 63 33 62 32 36 62 39 63 64 63 36 33  25ddc3b2 6b9cdc63
0070  63 62 35 66 34 32 38 30 39 38 38 38 32 39 64 63  cb5f4280 988829dc
0080  32 65 64 34 65 64 31 62 39 37 33 63 31 34 64 61  2ed4ed1b 973c14da
0090  30 64 32 36 64 38 61 35 35 35 63 39 33 64 31 32  0d26d8a5 55c93d12
00a0  33 31 34 62 30 37 63 34 31 64 31 66             314b07c4 1d1f

```

Windows Command Prompt:

```

Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khanh>echo Nguyen Quoc Khanh B20DCA
T103
Nguyen Quoc Khanh B20DCA T103

C:\Users\khanh>date
The current date is: Fri 05/12/2023
Enter the new date: (mm-dd-yy)

```