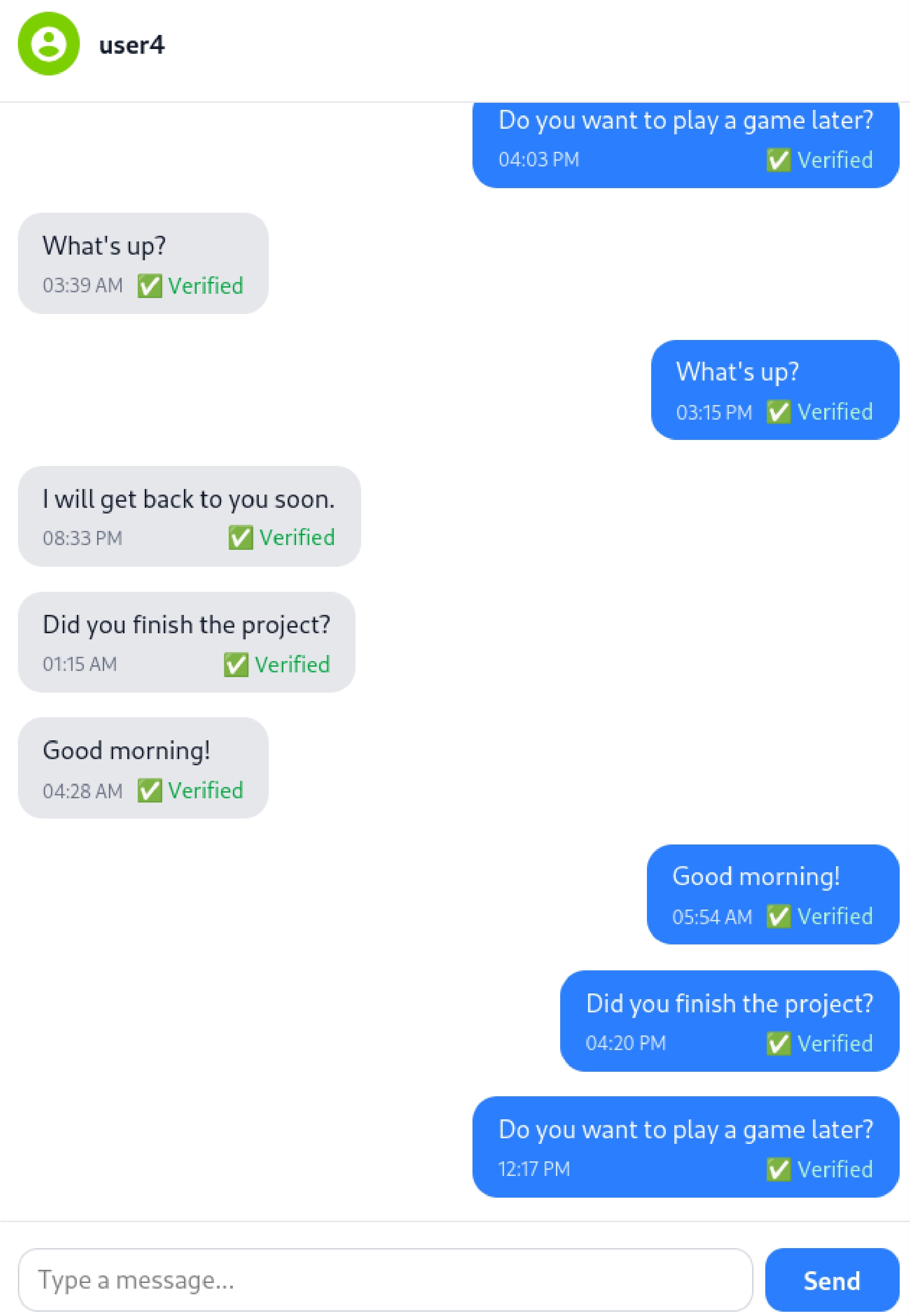
BAB III

Pengujian Program

3.1 Uji Digital Signature



user4

Do you want to play a game later?
04:03 PM ✅ Verified

What's up?
03:39 AM ✅ Verified

What's up?
03:15 PM ✅ Verified

I will get back to you soon.
08:33 PM ✅ Verified

Did you finish the project?
01:15 AM ✅ Verified

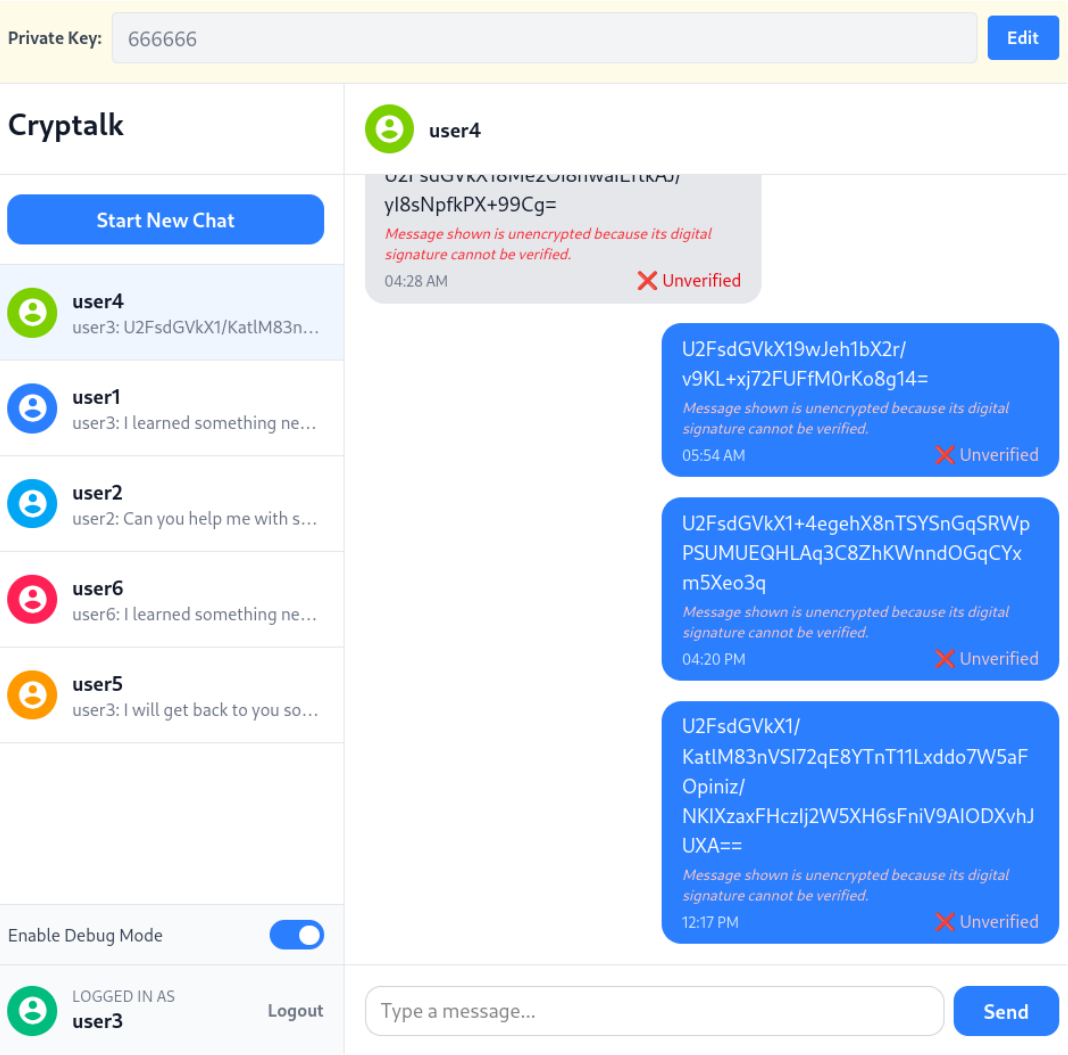
Good morning!
04:28 AM ✅ Verified

Good morning!
05:54 AM ✅ Verified

Did you finish the project?
04:20 PM ✅ Verified

Do you want to play a game later?
12:17 PM ✅ Verified

Gambar 3.1. *Tampilan chat history ketika private key masih benar*



Private Key: 666666

Cryptalk

user4
user3: U2FsdGVkX1/KatlM83n…

user1
user3: I learned something ne…

user2
user2: Can you help me with s…

user6
user6: I learned something ne…

user5
user3: I will get back to you so…

Enable Debug Mode

LOGGED IN AS
user3

user4

U2FsdGVkX18MeZOl8nwaiLrtkAJ/
yl8sNpfkPX+99Cg=
Message shown is unencrypted because its digital signature cannot be verified.
04:28 AM ❌ Unverified

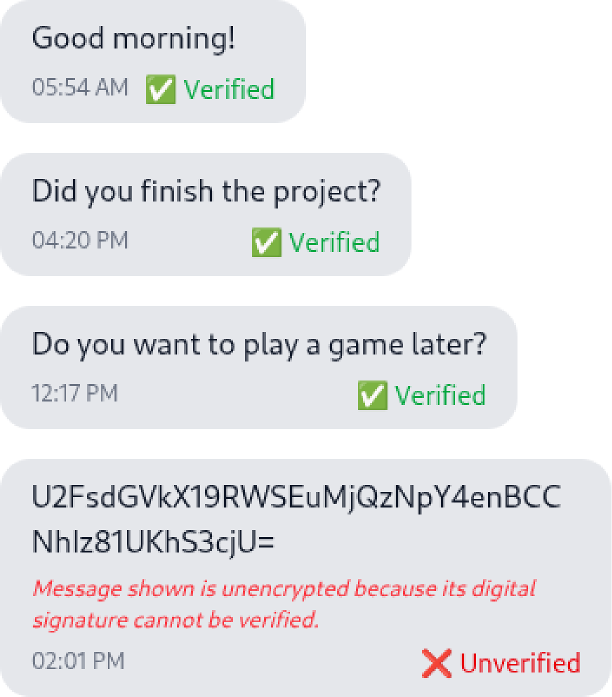
U2FsdGVkX19wJeh1bX2r/
v9KL+xj72FUFfM0rKo8g14=
Message shown is unencrypted because its digital signature cannot be verified.
05:54 AM ❌ Unverified

U2FsdGVkX1+4egehX8nTSYSnGqSRWp
PSUMUEQHLAq3C8ZhKWnndOGqCYx
m5Xeo3q
Message shown is unencrypted because its digital signature cannot be verified.
04:20 PM ❌ Unverified

U2FsdGVkX1/
KatlM83nVSI72qE8YTnT11Lxddo7W5aF
Opiniz/
NKIXzaxFHczIj2W5XH6sFniV9AIODXvhJ
UXA==
Message shown is unencrypted because its digital signature cannot be verified.
12:17 PM ❌ Unverified

Type a message...

Gambar 3.2. *Ketika private key diubah, seluruh pesan menjadi terenkripsi*



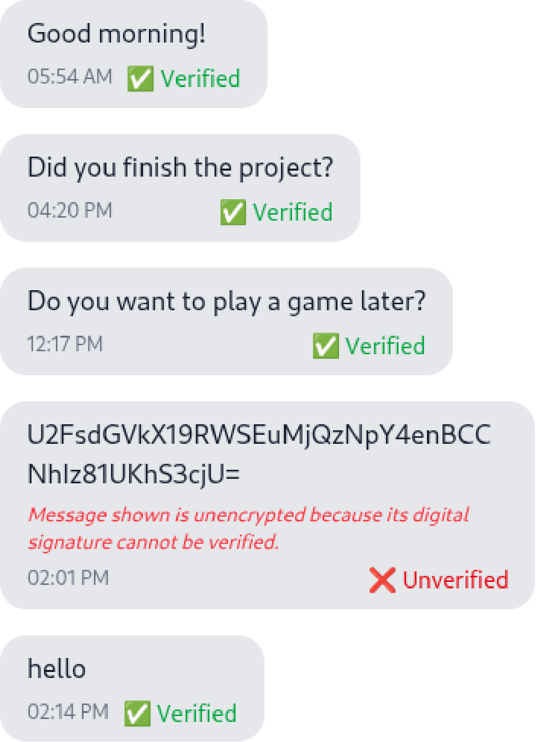
Good morning!
05:54 AM ✅ Verified

Did you finish the project?
04:20 PM ✅ Verified

Do you want to play a game later?
12:17 PM ✅ Verified

U2FsdGVkX19RWSEuMjQzNpY4enBCCNhlz81UKhS3cjU=
Message shown is unencrypted because its digital signature cannot be verified.
02:01 PM ❌ Unverified

Gambar 3.3. *Ketika pengguna tadi mengirim pesan, penerima menerima hasil terenkripsi dan dilabeli "Unverified"*



Good morning!
05:54 AM ✅ Verified

Did you finish the project?
04:20 PM ✅ Verified

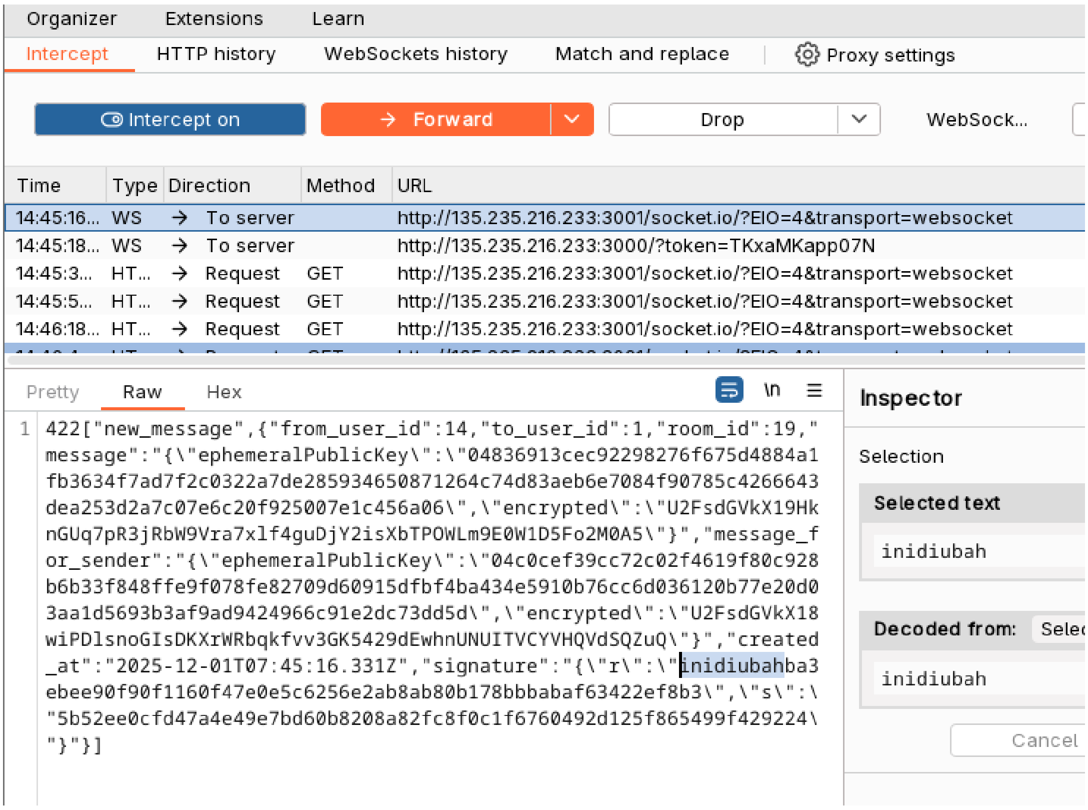
Do you want to play a game later?
12:17 PM ✅ Verified

U2FsdGVkX19RWSEuMjQzNpY4enBCCNhlz81UKhS3cjU=
Message shown is unencrypted because its digital signature cannot be verified.
02:01 PM ❌ Unverified

hello
02:14 PM ✅ Verified

Gambar 3.4 *Ketika private key sudah dibenarkan, pesan selanjutnya terverifikasi, tapi pesan sebelumnya masih terenkripsi*

3.2 Uji *Intercept*



Time	Type	Direction	Method	URL
14:45:16...	WS	→ To server		http://135.235.216.233:3001/socket.io/?EIO=4&transport=websocket
14:45:18...	WS	→ To server		http://135.235.216.233:3000/?token=TKxaMKapp07N
14:45:3...	HT...	→ Request	GET	http://135.235.216.233:3001/socket.io/?EIO=4&transport=websocket
14:45:5...	HT...	→ Request	GET	http://135.235.216.233:3001/socket.io/?EIO=4&transport=websocket
14:46:18...	HT...	→ Request	GET	http://135.235.216.233:3001/socket.io/?EIO=4&transport=websocket

```
422["new_message",{"from_user_id":14,"to_user_id":1,"room_id":19,"
message":"{\"ephemeralPublicKey\":\"04836913cec92298276f675d4884a1
fb3634f7ad7f2c0322a7de285934650871264c74d83aeb6e7084f90785c4266643
dea253d2a7c07e6c20f925007e1c456a06\",\"encrypted\":\"U2FsdGVkX19Hk
nGUq7pR3jRbW9Vra7xlf4guDjY2isXbTPOWLm9E0W1D5Fo2M0A5\"}","message_f
or_sender":"{\"ephemeralPublicKey\":\"04c0cef39cc72c02f4619f80c928
b6b33f848ffe9f078fe82709d60915dfbf4ba434e5910b76cc6d036120b77e20d0
3aa1d5693b3af9ad9424966c91e2dc73dd5d\",\"encrypted\":\"U2FsdGVkX18
wiPDlsnoGIsDKXrWRbqkfvv3GK5429dEwhnUNUITVCYVHQVdSQZuQ\"}","created
_at":"2025-12-01T07:45:16.331Z","signature":"{\"r\":\"inidiubahba3
ebee90f90f1160f47e0e5c6256e2ab8ab80b178bbbabaf63422ef8b3\",\"s\":\
"5b52ee0cfd47a4e49e7bd60b8208a82fc8f0c1f6760492d125f865499f429224\
"}"}]
```

Inspector

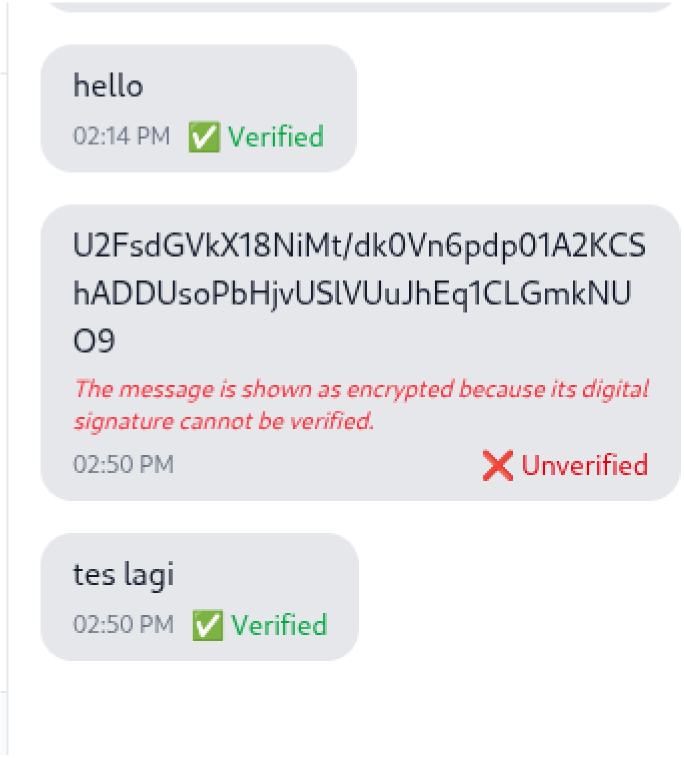
Selection

Selected text: inidiubah

Decoded from: Selec

inidiubah

Gambar 3.5. *Paket di-intercept menggunakan Burp Suite dan digital signature dimodifikasi*



hello

02:14 PM ✅ Verified

U2FsdGVkX18NiMt/dk0Vn6pdp01A2KCShADDUsoPbHjvUSlVUuJhEq1CLGmkNUO9

The message is shown as encrypted because its digital signature cannot be verified.

02:50 PM ❌ Unverified

tes lagi

02:50 PM ✅ Verified

Gambar 3.6. *Pesan yang di-intercept terenkripsi dan dilabeli "Unverified"*