

Лабораторна робота №6

Виконав: Ваврикович Михайло ПМІ-33

Тема: Протокол обміну ключами Діффі-Гелмана

Мета: Реалізувати протокол обміну ключами Діффі-Гелмана

Хід роботи

1. Розробив протокол обміну ключами Діффі-Гелмана

Diffie-Hellman key exchange

P value

G value

a Private key value b Private key value

a Public key value b Public key value

s Private key value

Get private key S

```

src > components > containers > DiffieHellman > index.tsx > DiffieHellman
5 import { Button, InputNumber } from '@components/UI/atoms';
6 import { modPow } from '@utils';
7
8 type DiffieHellmanForm = {
9   gValue: number;
10  pValue: number;
11  aPrivateKey: number;
12  bPrivateKey: number;
13  aPublicKey: number;
14  bPublicKey: number;
15  sPrivateKey: number;
16 };
17
18 const DiffieHellman: FC = () => {
19   const [form] = useForm<DiffieHellmanForm>();
20
21   const { number } = useFormFieldSchema();
22   const schema = useYupSchema({
23     gValue: number,
24     pValue: number,
25     aPrivateKey: number,
26     bPrivateKey: number,
27   });
28
29   const generatePrivateKey = useCallback(() => {
30     const { gValue, pValue, aPrivateKey, bPrivateKey } = form.getFieldsValue();
31
32     const aPublicKey = modPow(gValue, aPrivateKey, pValue);
33     const bPublicKey = modPow(gValue, bPrivateKey, pValue);
34
35     form.setFieldsValue({
36       aPublicKey,
37       bPublicKey,
38       sPrivateKey: modPow(bPublicKey, aPrivateKey, pValue),
39     });
40   }, [form]);

```

Висновок: я реалізував протокол обміну ключами Діффі-Гелмана