Реалізація основних асиметричних криптосистем

Encode data:

```
$ echo -n hello crypto | base64
aGVsbG8gY3J5cHRv
```

Run server:

```
$ python3 app2.py
 * Serving Flask app 'app2'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production
deployment. Use a production WSGI server instead.
 * Running on https://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with watchdog (inotify)
 * Debugger is active!
 * Debugger PIN: 786-824-269
```

Send request to sign data:

```
$ $ curl -X POST https://127.0.0.1:5000/v1/sign -d
'{"data":"aGVsbG8gY3J5cHRv"}' -H "Content-Type: application/json" -k
{
  "signature":
"KStpNa1Ke5UAqKDW4xqWRA5J+LFaErfm7wHNvUy+iklGPElG3QSIabDt3Pml2MaKVsCacfsT
4LRBqDtUmPv7YFKUlrjwrEjQ58b/igvQZmJxL37OFLhH/G3HpLj2+nHot+wiC3dsCXj/uj6Na
ZK5OfD45GuLkVHvNUrE5ecrhSYN4CCyyBLj3sSIbVWL+9Op1aqLjBdZ+U1Z+15IhSK6TfM5gA
RJT63Dro+bvzVP7xq58G4ktLm39mHwvM0aOsr3uvvJ0TcM1q2zl9mvqBDwRmYXwFzNEBLTkSB
8Np8/ULbPwcWYRTiB82Al/6qhWhDjHfcJEPptCswV3MEzIRsB6w=="
}
```

Send request to verify signature:

```
$ curl -X POST https://127.0.0.1:5000/v1/verify -d
'{"data":"aGVsbG8gY3J5cHRv",
"signature":"KStpNa1Ke5UAqKDW4xqWRA5J+LFaErfm7wHNvUy+iklGPElG3QSIabDt3Pml
```

```
2MaKVsCacfsT4LRBqDtUmPv7YFKUlrjwrEjQ58b/igvQZmJxL37OFLhH/G3HpLj2+nHot+wiC
3dsCXj/uj6NaZK5OfD45GuLkVHvNUrE5ecrhSYN4CCyyBLj3sSIbVWL+9Op1aqLjBdZ+U1Z+1
5IhSK6TfM5gARJT63Dro+bvzVP7xq58G4ktLm39mHwvM0aOsr3uvvJ0TcM1q2zl9mvqBDwRmY
XwFzNEBLTkSB8Np8/ULbPwcWYRTiB82Al/6qhWhDjHfcJEPptCswV3MEzIRsB6w==}' -H
"Content-Type: application/json" -k
{
  "verified": true
}
```

Tests with invalid and empty signature:

```
$ curl -X POST https://127.0.0.1:5000/v1/verify -d
'{"data":"aGVsbG8gY3J5cHRv", "signature":"zIRs"}' -H "Content-Type:
application/json" -k
{
  "verified": false
}

$ curl -X POST https://127.0.0.1:5000/v1/verify -d
'{"data":"aGVsbG8gY3J5cHRv"}' -H "Content-Type: application/json" -k
{
  "error": "Missing data or signature"
}
```

Server logs:

```
127.0.0.1 - - [27/Dec/2023 21:26:12] "POST /v1/sign HTTP/1.1" 200 -
127.0.0.1 - - [27/Dec/2023 21:26:41] "POST /v1/verify HTTP/1.1" 200 -
127.0.0.1 - - [27/Dec/2023 21:26:47] "POST /v1/verify HTTP/1.1" 200 -
127.0.0.1 - - [27/Dec/2023 21:27:56] "POST /v1/verify HTTP/1.1" 200 -
127.0.0.1 - - [27/Dec/2023 21:28:11] "POST /v1/verify HTTP/1.1" 400 -
```