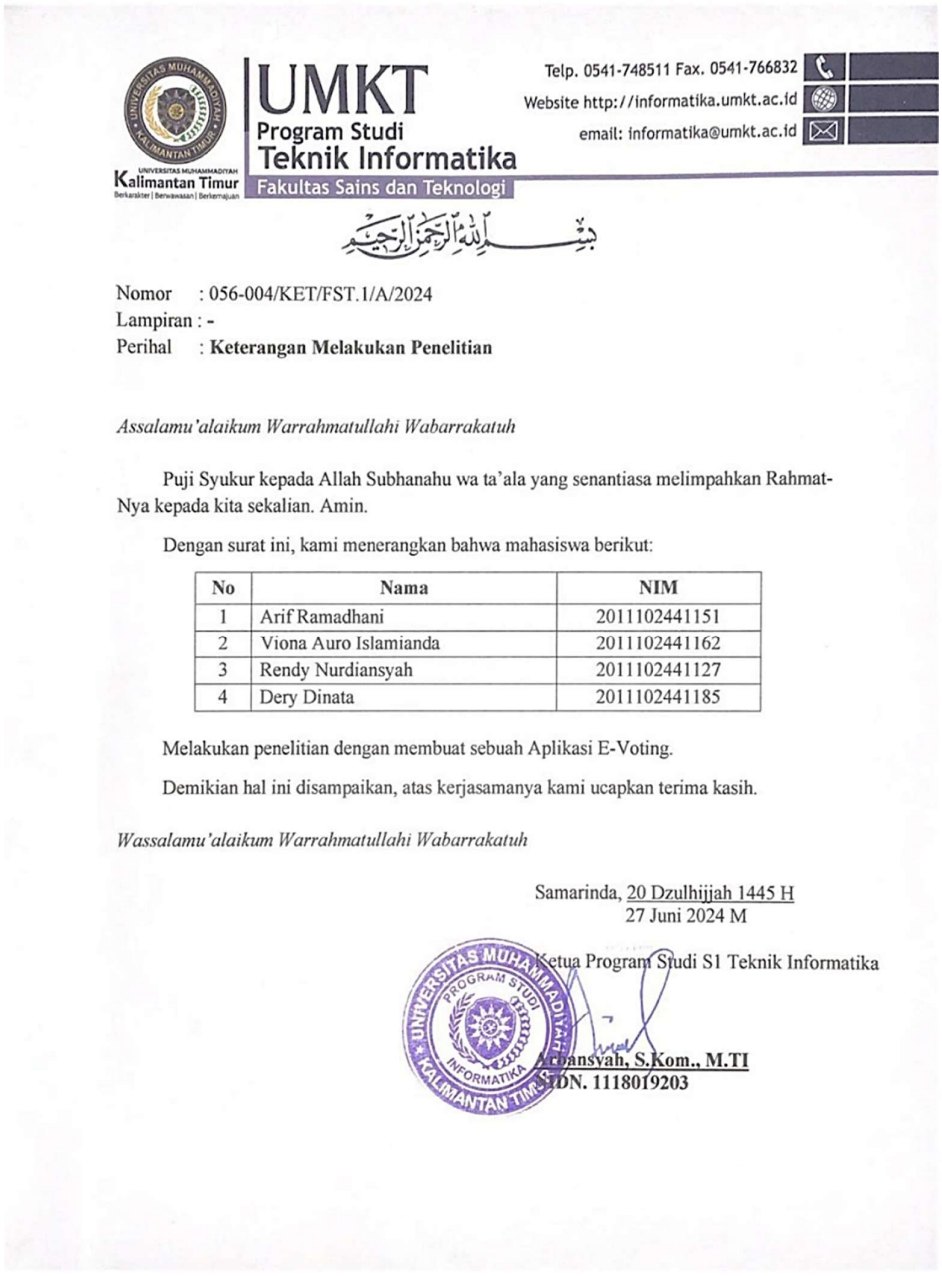
LAMPIRAN

Lampiran 1. Jadwal Penelitian

NO	Jenis Penelitian	Bulan/2024					
		Feb	Maret	April	Mei	Juni	Juli
Tahap Pra Penelitian							
1	Menentukan Judul Penelitian						
2	Mengidentifikasi Permasalahan						
3	Menyusun Metode Penelitian						
4	Menentukan Studi Kasus						
5	Menyusun Proposal Penelitian						
6	Review Desk Simpel						
Tahap Penelitian							
1	Analisis Kebutuhan						
2	Desain Perancangan						
3	Implementasi Keamanan						
4	Pengujian						
5	Kesimpulan						
Tahap Akhir Penelitian							
1	Penyusunan laporan						
2	Seminar Hasil						

Lampiran 2. SK Melakukan Penelitian



UMKT
Program Studi
Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Muhammadiyah Kalimantan Timur
Berkarakter | Berwawasan | Berkemajuan

Telp. 0541-748511 Fax. 0541-766832
Website http://informatika.umkt.ac.id
email: informatika@umkt.ac.id

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Nomor : 056-004/KET/FST.1/A/2024
Lampiran : -
Perihal : **Keterangan Melakukan Penelitian**

Assalamu'alaikum Warrahmatullahi Wabarrakatuh

Puji Syukur kepada Allah Subhanahu wa ta'ala yang senantiasa melimpahkan Rahmat-Nya kepada kita sekalian. Amin.

Dengan surat ini, kami menerangkan bahwa mahasiswa berikut:

No	Nama	NIM
1	Arif Ramadhani	2011102441151
2	Viona Auro Islamianda	2011102441162
3	Rendy Nurdiansyah	2011102441127
4	Dery Dinata	2011102441185

Melakukan penelitian dengan membuat sebuah Aplikasi E-Voting.

Demikian hal ini disampaikan, atas kerjasamanya kami ucapkan terima kasih.

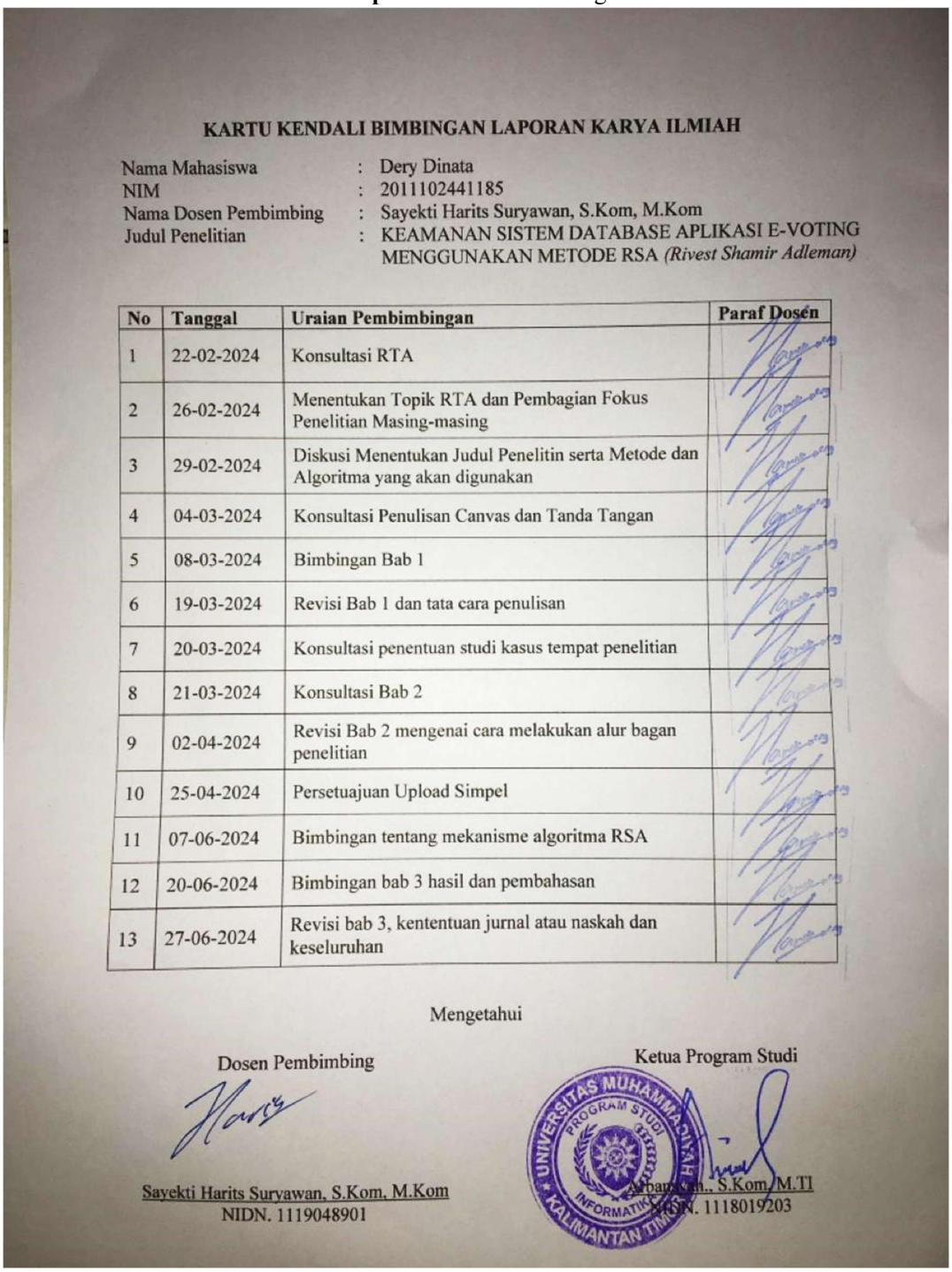
Wassalamu'alaikum Warrahmatullahi Wabarrakatuh

Samarinda, 20 Dzulhijjah 1445 H
27 Juni 2024 M

Ketua Program Studi S1 Teknik Informatika

Rendy Nurdiansyah, S.Kom., M.TI
NIDN. 1118019203

Lampiran 3. Kartu Bimbingan



KARTU KENDALI BIMBINGAN LAPORAN KARYA ILMIAH

Nama Mahasiswa : Dery Dinata
NIM : 2011102441185
Nama Dosen Pembimbing : Sayekti Harits Suryawan, S.Kom, M.Kom
Judul Penelitian : KEAMANAN SISTEM DATABASE APLIKASI E-VOTING MENGGUNAKAN METODE RSA *(Rivest Shamir Adleman)*

No	Tanggal	Uraian Pembimbingan	Paraf Dosen
1	22-02-2024	Konsultasi RTA	
2	26-02-2024	Menentukan Topik RTA dan Pembagian Fokus Penelitian Masing-masing	
3	29-02-2024	Diskusi Menentukan Judul Penelitin serta Metode dan Algoritma yang akan digunakan	
4	04-03-2024	Konsultasi Penulisan Canvas dan Tanda Tangan	
5	08-03-2024	Bimbingan Bab 1	
6	19-03-2024	Revisi Bab 1 dan tata cara penulisan	
7	20-03-2024	Konsultasi penentuan studi kasus tempat penelitian	
8	21-03-2024	Konsultasi Bab 2	
9	02-04-2024	Revisi Bab 2 mengenai cara melakukan alur bagan penelitian	
10	25-04-2024	Persetuajuan Upload Simpel	
11	07-06-2024	Bimbingan tentang mekanisme algoritma RSA	
12	20-06-2024	Bimbingan bab 3 hasil dan pembahasan	
13	27-06-2024	Revisi bab 3, kententuan jurnal atau naskah dan keseluruhan	

Mengetahui

Dosen Pembimbing

Sayekti Harits Suryawan, S.Kom, M.Kom
NIDN. 1119048901

Ketua Program Studi

Arbanowati, S.Kom, M.TI
NIDN. 1118019203

Lampiran 4. Wawancara Narasumber Organisasi HIMATIKA

Lampiran 5. Wawancara Narasumber Organisasi UKM Pencak Silat

Lampiran 6. Hasil Wawancara

No	Pertanyaan	Narasumber 1	Narasumber 2	Narasumber 3	Narasumber 4
1	Apa peran Anda dalam organisasi interkampus?	Ketua Himatika	Anggota Himatika	Anggota UKM Silat	Wakil UKM Silat dan Kordinator Pelatih
2	Bagaimana biasanya proses pemilihan dilakukan di organisasi Anda?	Menggunakan pemungutan suara manual dan penghitungan langsung	Menggunakan pemungutan suara manual dan penghitungan langsung	Menggunakan pemungutan suara manual dan penghitungan langsung	Menggunakan pemungutan suara manual dan penghitungan langsung
3	Apa tantangan terbesar yang Anda hadapi dengan proses pemilihan saat ini?	Proses penghitungan suara yang memakan waktu dan dan kurang efisien	Proses penghitungan suara yang memakan waktu dan dan kurang efisien	Proses penghitungan suara yang memakan waktu dan dan kurang efisien	Proses penghitungan suara yang memakan waktu dan dan kurang efisien
4	Apa saja kelebihan dari proses pemilihan saat ini yang ingin Anda pertahankan dalam sistem E-voting?	Kelebihannya dalam akurasinya yang tepat	Kelebihannya dalam akurasinya yang tepat	Kelebihannya dalam akurasinya yang tepat	Kelebihannya dalam akurasinya yang tepat
5	Fitur apa yang menurut Anda paling penting dalam aplikasi E-voting?	Antarmuka yang mudah digunakan	Keamanan dan validitas suara	Antarmuka yang mudah digunaka dan aman digunakan	Antarmuka yang mudah digunaka dan aman digunakan
6	Bagaimana Anda ingin proses pendaftaran pemilih dilakukan?	Yang mendaftar adalah anggota aktif sesuai peraturan organisasi	Yang mendaftar adalah anggota aktif sesuai peraturan organisasi	Yang mendaftar adalah anggota aktif sesuai peraturan organisasi	Yang mendaftar adalah anggota aktif sesuai peraturan organisasi
7	Bagaimana menurut Anda sistem verifikasi identitas pemilih harus dilakukan?	Yang berhak memilih adalah anggota aktif dari organisasi dan ukm	Yang berhak memilih adalah anggota aktif dari organisasi dan ukm	Yang berhak memilih adalah anggota aktif dari organisasi dan ukm	Yang berhak memilih adalah anggota aktif dari organisasi dan ukm

No	Pertanyaan	Narasumber 1	Narasumber 2	Narasumber 3	Narasumber 4
8	Apakah Anda membutuhkan fitur pemantauan real-time untuk hasil pemilihan?	Sepertinya Tidak perlu hasilnya keluar saat pemilihan selesai saja	Sepertinya Tidak perlu hasilnya keluar saat pemilihan selesai saja	Sepertinya Tidak perlu hasilnya keluar saat pemilihan selesai saja	Sepertinya Tidak perlu hasilnya keluar saat pemilihan selesai saja
9	Apa saja kekhawatiran Anda terkait keamanan dalam E-voting?	Risiko peretasan dan manipulasi hasil	Keamanan data pemilih dan hasil pemilihan	Privasi dan anonimitas pemilih	Keamanan data pemilih dan hasil pemilihan
10	Seberapa penting bagi Anda bahwa hasil pemilihan tidak dapat diubah setelah pemungutan suara selesai?	Sangat penting, untuk menjaga integritas proses voting	Penting karena seharusnya pemilih wajib Cuma menggunakan 1 suara	Penting karena seharusnya pemilih wajib Cuma menggunakan 1 suara	Penting karena seharusnya pemilih wajib Cuma menggunakan 1 suara
11	Bagaimana Anda ingin sistem menangani pemilih yang mencoba memberikan suara lebih dari sekali?	Pemilih hanya boleh menggunakan satu ID untuk satu suara	Pemilih hanya boleh menggunakan satu ID untuk satu suara	Pemilih hanya boleh menggunakan satu ID untuk satu suara	Pemilih hanya boleh menggunakan satu ID untuk satu suara
12	Seberapa mudah Anda ingin proses pemilihan dalam aplikasi ini?	Sangat mudah	Mudah dan proses yang sederhana	Mudah dimengerti oleh semua pemilih	Mudah digunakan

Lampiran 7 Surce Code Pembangkiat Kunci

```python
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import base64
import logging

logger = logging.getLogger(__name__)

def generate_rsa_keys(pemilih_id):
    key = RSA.generate(2048)
    private_key = key.export_key()
    public_key = key.publickey().export_key()

    # Save private key to file
    private_key_path = f'static/keys/private_key_rsa_{pemilih_id}.pem'
    with open(private_key_path, 'wb') as f:
        f.write(private_key)

    # Save public key to file
    public_key_path = f'static/keys/public_key_rsa_{pemilih_id}.pem'
    with open(public_key_path, 'wb') as f:
        f.write(public_key)

def load_rsa_private_key(pemilih_id):
    private_key_path = f'static/keys/private_key_rsa_{pemilih_id}.pem'
    with open(private_key_path, 'rb') as f:
        private_key = RSA.import_key(f.read())
    return private_key

def load_rsa_public_key(pemilih_id):
    public_key_path = f'static/keys/public_key_rsa_{pemilih_id}.pem'
    with open(public_key_path, 'rb') as f:
        public_key = RSA.import_key(f.read())
    return public_key
```

Lampiran 8 Source Code Enkripsi

```python
            # untuk mengenkripsi RSA
            public_key_rsa = load_rsa_public_key(pemilih_id)
            encrypted_nama_pemilih = encrypt_with_public_key(public_key_rsa.export_key(), pemilih.nama)
            encrypted_nama_kandidat = encrypt_with_public_key(public_key_rsa.export_key(), kandidat.nama)
            encrypted_judul_pemilihan = encrypt_with_public_key(public_key_rsa.export_key(), pemilihan.judul)
            waktu_voting = datetime.now()

            # simpan suara
            voting = Voting(
                nama_pemilih=encrypted_nama_pemilih,
                nama_kandidat=encrypted_nama_kandidat,
                judul_pemilihan=encrypted_judul_pemilihan,
                waktu_voting=waktu_voting
            )
            voting.save()
```

Lampiran 9 Source Code Dekripsi

```python
    for vote in voting_results:
        decrypted = False
        for pemilih_id in pemilih_ids:
            private_key_rsa = load_rsa_private_key(pemilih_id)
            try:
                decrypted_nama_kandidat = decrypt_with_private_key(private_key_rsa, vote.nama_kandidat).strip()
                decrypted_nama_pemilih = decrypt_with_private_key(private_key_rsa, vote.nama_pemilih).strip()
                decrypted_judul_pemilihan = decrypt_with_private_key(private_key_rsa, vote.judul_pemilihan).strip()

                logger.debug(f"Decrypted kandidat: {decrypted_nama_kandidat}")
                logger.debug(f"Decrypted pemilih: {decrypted_nama_pemilih}")
                logger.debug(f"Decrypted pemilihan: {decrypted_judul_pemilihan}")

                # Only count votes that match the current pemilihan
                if decrypted_judul_pemilihan == pemilihan.judul:
                    if decrypted_nama_kandidat in vote_counts:
                        vote_counts[decrypted_nama_kandidat] += 1
                    else:
                        vote_counts[decrypted_nama_kandidat] = 1

                    decrypted = True
                    break
            except Exception as e:
                logger.error(f"Error decrypting vote for vote ID {vote.id} with pemilih ID {pemilih_id}: {str(e)}")
                continue
        if not decrypted:
            logger.error(f"Error decrypting vote for vote ID {vote.id}: Unable to decrypt with any pemilih private key")
```

Lampiran 10. *Source Code* Pengujian Fungsional

```
from cryptography.hazmat.primitives.asymmetric import rsa

from cryptography.hazmat.primitives.asymmetric import padding

from cryptography.hazmat.primitives import hashes

from cryptography.hazmat.primitives import serialization


# Fungsi untuk membuat kunci RSA

def buat_kunci():

    kunci_privat = rsa.generate_private_key(

        public_exponent=65537,

        key_size=2048,

    )

    kunci_publik = kunci_privat.public_key()

    return kunci_privat, kunci_publik


# Fungsi untuk mengenkripsi data dengan kunci publik

def enkripsi_data(kunci_publik, data):

    ciphertext = kunci_publik.encrypt(

        data,

        padding.OAEP(

            mgf=padding.MGF1(algorithm=hashes.SHA256()),

            algorithm=hashes.SHA256(),

            label=None

        )

    )

    return ciphertext
```

```
# Fungsi untuk mendekripsi data dengan kunci privat
def dekripsi_data(kunci_privat, ciphertext):
    plaintext = kunci_privat.decrypt(
        ciphertext,
        padding.OAEP(
            mgf=padding.MGF1(algorithm=hashes.SHA256()),
            algorithm=hashes.SHA256(),
            label=None
        )
    )
    return plaintext

# Fungsi untuk menampilkan kunci dalam format PEM
def tampilkan_kunci(kunci_privat, kunci_publik):
    kunci_privat_pem = kunci_privat.private_bytes(
        encoding=serialization.Encoding.PEM,
        format=serialization.PrivateFormat.PKCS8,
        encryption_algorithm=serialization.NoEncryption()
    ).decode('utf-8')

    kunci_publik_pem = kunci_publik.public_bytes(
        encoding=serialization.Encoding.PEM,
        format=serialization.PublicFormat.SubjectPublicKeyInfo
    ).decode('utf-8')

    print("Kunci Privat:")
```

```
    print(kunci_privat_pem)
    print("Kunci Publik:")
    print(kunci_publik_pem)

# Fungsi utama untuk pengujian
def utama():
    # Membuat kunci
    kunci_privat, kunci_publik = buat_kunci()

    # Menampilkan kunci
    tampilkan_kunci(kunci_privat, kunci_publik)

    # Data asli yang akan dienkripsi
    data_asli = b"dery dinata"

    # Mengenkripsi data
    data_enkripsi = enkripsi_data(kunci_publik, data_asli)
    print(f"Data terenkripsi: {data_enkripsi}")

    # Mendekripsi data
    data_dekripsi = dekripsi_data(kunci_privat, data_enkripsi)

    # Simulasikan ketidaksesuaian data dengan mengubah data asli untuk verifikasi
    # data_asli_baru = b"Data ini sudah diubah."

    # Cetak data yang didekripsi
```

```
    print(f"Data terdekripsi: {data_dekripsi}")


    # Memastikan data terdekripsi sama dengan data asli (dengan ketidaksesuaian)
    # try:
    #     assert data_dekripsi == data_asli_baru, "Dekripsi gagal, data tidak cocok!"
    print("Dekripsi berhasil, data cocok!")
    # except AssertionError as e:
    #     print(e)


if __name__ == "__main__":
    utama()
```

Lampiran 11. Output Hasil Pengujian Fungsionalitas

```
PS C:\Users\MSI USER\OneDrive\Documents\kriptoRSA\evoting> & "C:/Users/MSI
USER/AppData/Local/Programs/Python/Python312/python.exe" "c:/Users/MSI
USER/OneDrive/Documents/kriptoRSA/evoting/dashboard/coba.py"
Kunci Privat:
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDG+KOjKf+nBTiF
teXWpmT7gwSZ91p+EVuuSJ8AO0DGhmPslHqkSWJmVu69w5sa9Rt2qIkU8gy8+7lZ
98ZUehPnOH4z9GSJYdVQbQL/9hiEM3qIuZplunLFxkFxxEGXT6udMet1sBWj46JQ
h7ILzm61F9OcU/OzIJkZI5ifPSs11b/du2vNj+C7ocbbZUyv3qYYEBV49DkFg0t+
Ehww6mOJZY56k9kyiq/wuN24YLpYV/ZrhQ1HKptxjEywbv6IBoeEpmN/97U7w6is
v5Og7/eBW2Xp7PrCnwusftbD08SPVPqGgfcR+npmvTAH1APqZ/Pq1D89/dFLaEKE
heqqFOGTAgMBAAECggEAJMVLfHplAClTVkaU6LPMgrymS4vuYdD0aAOMut64bFfm
vJB+D8FuGWqkaVZuYi98+VNRLhlDaGN+0BUdxnvfFMKYdCKMt+ToJppWzRXeVwQq
d30Rfw5TaqBmdM9nrb5wATd6A8BcZ3LIiuhg65SlWftCxKexKF/0WzR8XqVPyH1a
IMwsXdq4xXLplQOFnBnMYJr9NAuUWbb+wEHUNrARJlK/g+s0glLEg3FbPU8ct76A
```

+JU8FvrKrAcJkRuG0fpYUVYMeikkF93mUt/hkZ5mjEzqVMWOBYmoRZZMnDOxaDHT

CVWwU6LiVmf7Przc5mc8bMnjSorpQQ6v7AUf4Hm1lQKBgQDrAbWZpbmrk8oSar4W

a+VSpQfZN37LO7IeuRk75EFGiUfReolPUKSx6FaSngYvcSktd9oz4MS4D3SfWPma

M3gBeJSRH5sslJX/iBTGBkmNKZ05ycZ7pRNpxjYWyCKVoPzwhlRmXZJvpgFILtH1

2oj3oMCUJdq3GVpAQ3szjiK3NwKBgQDYvtju5ARbg/w1KmGYSRSX1FFXbS9faLTq

X3tCjdyzj6jFF5KOamqA0tt/0KGVUOevs7EtE5tsxDoTUwSQgaNpRqSUWHxGrztP

p3q3wlMh4Y5z9JxW3mUisTqdoAPLc9Gab8QDuZy582cvhLYuVRzeFYuApGh6YTvN

avy0IybehQKBgEIRy/Vzczy6oxAEdIanNOTEQu2dvYbztIMQtPhylqt3AvrwwVPM

L1FZKaW0ybZi0RnYXT9CjOvWZIo8IIhque1n8hTO1vh0masqnfSCZgFK1sodYTD3

2vpc4G4NPDPm+9W/XlEdM4MyH6AkkaDWHLXJuvqrnc7mUMpKboOzDS2HAoGBAKon

QPRhis4xUjiGmfFMRd9fra+9pnf3IjfwVzqLVdydBfgcJlCpWAzj+69eoMswpYH4

xjnF77k2XwU2ohmzvA50h9VxlbaD8EL7DsrdwheSFBwRxv4nPyw6B/MgYHpC5SSh

Yzctas1MORBD1iWPaccrEMYfy2lvldwQhmwAQI5lAoGAbGXtUCJbExqjJ4DrIyt4

jXBaUYppv1VhyHnl3TcGSORRusM/u/jMen5OIIhgPF24lGh0AyBu+r3KHuZt9HNt

UpzXHsu3QXW2wRFdTbTbzceVFY+mu4+tpRuU4yWMCBwE7ghNZ2JbagRHV4n3Aon5

I2UU+VGmgYiVLyTNDR8acfY=

-----END PRIVATE KEY-----

Kunci Publik:

-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxvijoyn/pwU4hbXl1qZk

+4MEmfdafhFbrkifADtAxoZj7JR6pEliZlbuvcObGvUbdqiJFPIMvPu5WffGVHoT

5zh+M/RkiWHVUG0C//YYhDN6iLmaZbpyxcZBccRBl0+rnTHrdbAVo+OiUIeyC85u

tRfTnFPzsyCZGSOYnz0rNdW/3btrzY/gu6HG22VMr96mGBAVePQ5BYNLfhIcMOpj

iWWOepPZMoqv8LjduGC6WFf2a4UNRyqbcYxMsG7+iAaHhKZjf/e1O8OorL+ToO/3

gVtl6ez6wp8LrH7Ww9PEj1T6hoH3Efp6Zr0wB9QD6mfz6tQ/Pf3RS2hChIXqqhTh

kwIDAQAB

-----END PUBLIC KEY-----

Data terenkripsi:
b'n\xd5\x9f\x80\xca\xe3F\xb4\xef\xac\xa6@+\x13|\xf7;!\x1e?\xb5\x10\x9bP"S\xbd\x9d\xbd\xe9\xb0\
xe6\x04\x95L&\x08\xfa\x92\x1e\x02\xe3\xdfm\xa0\xda\n
\xa5\xa2\xd8V\x1a\xbe$\xd2\xfcw\x12\xe3f\xfb/A\x94G\x9c\xae\xd8Ab.\xfb\x139\xc4t\xf40\xde\n\x
0f}\xcfo\x11{?\xf9\xdf\xe7y\xf4\xe9\xd9\x8d\xc8A9B\xef~\xc1\x97\xac\xd0\x9e\xces\xe2\xac\xcb\xf
6\xdcOG-
\xd2\xf2\xb4\xd1\xaa\xd7\xc9\x13P\xad\xf0\x8er\x1a2Zf\xc6\xe00&\xd8\x9e\xfc\xe1\xe6g\xe5\x12\x
16\r\xe3)\x94\xeb\x81e\xff\x12\xee\xe1f\x99\xb7U\xf0\xc0MM\xd7z\x9e\x88\xe7oVx\x1e0\xbd\x9a=
\xb0g\xff\xe6En\xe0*+t\xc4\xfa\xe3\xc7\xc0\xb5\xd1\x9ag\xea03\xea\xc0\x95o\x83X\xb5Ro\xc8P\n\
xe7%\xa0\xbbKz\xdfG\x940\x9fX\x0bVG\xd6<\x04z\xb64\xbaZ\x07=\x93~\xe4\xcdY\xdd}\xae\x87\
xdb\xd3j\xb4\xad\xd1\x8a\xe5\xee'

Data terdekripsi: b 'dery dinata'

Dekripsi berhasil, data cocok!