Nama: Salsabila Wali Datussyuhada

NPM: 20123017

Kelas: C1.23

LAPORAN TUGAS 2

Algoritma Modern

1. Pendahuluan

Algoritma modern seperti AES, RSA, hash functions, dan digital signature merupakan fondasi utama dalam keamanan informasi. Pada tugas ini dilakukan implementasi nyata algoritma tersebut untuk memahami cara kerja, karakteristik, dan tingkat keamanannya dalam praktik.

2. Implementasi dan Analisis

2.1 AES (Advanced Encryption Standard)

AES adalah cipher **symmetric-key** yang menggunakan blok 128-bit.
Pada implementasi ini digunakan mode **CBC**, karena lebih aman dari ECB.
Hasil pengujian menunjukkan:

- Enkripsi menghasilkan ciphertext unik setiap proses (karena IV random)
- Dekripsi selalu mengembalikan plaintext asli

Kelemahan CBC → membutuhkan padding & IV harus dikirim bersama ciphertext.

2.2 RSA (Rivest–Shamir–Adleman)

RSA adalah algoritma **asymmetric-key**.
Langkah kerja:

1. Generate kunci publik & privat (2048-bit).
2. Enkripsi dilakukan dengan public key.
3. Dekripsi dengan private key.

Hasil percobaan:

- RSA aman untuk pesan pendek
- Tidak cocok untuk file besar → digunakan untuk enkripsi kunci AES (hybrid)

2.3 Hash Functions (MD5, SHA-1, SHA-256)

Algoritma	Panjang Output	Keamanan
MD5	128-bit	Rentan collision
SHA-1	160-bit	Rentan collision
SHA-256	256-bit	Sangat aman

Hasil hashing selalu *irreversible* dan berubah total bila ada 1 karakter berubah (*avalanche effect*).

2.4 Digital Signature (SHA-256 + RSA)

Digital signature memastikan:

- **Integrity** (data tidak berubah)
- **Authenticity** (pembuat dapat diverifikasi)
- **Non-repudiation**

Proses:

1. Melakukan hashing pada pesan.
2. Hash ditandatangani menggunakan private key.
3. Verifikasi menggunakan public key.

Hasil: verifikasi selalu valid selama pesan tidak diubah.

3. Eksperimen & Hasil

- Semua program berjalan baik pada Python + PyCryptodome.
- AES menghasilkan ciphertext berbeda setiap eksekusi.
- RSA berjalan lambat jika data terlalu besar.

- Signature dapat mendeteksi modifikasi 1 karakter sekalipun.

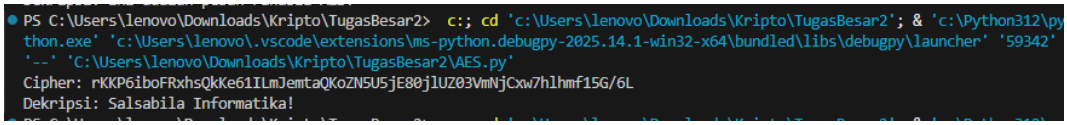
4. Analisis Keamanan

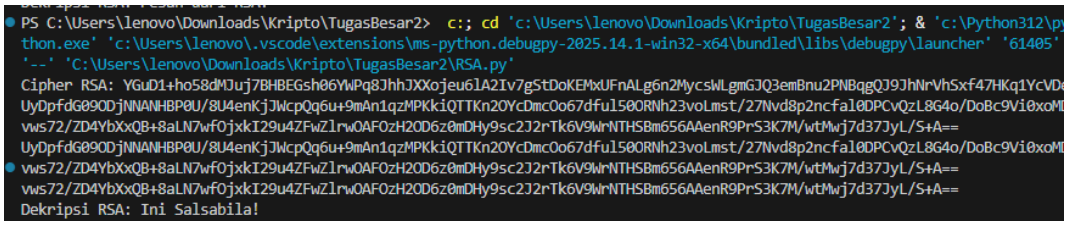
- AES-CBC aman, tetapi mode GCM lebih baik (authenticated encryption).
- RSA 2048-bit aman untuk penggunaan saat ini.
- SHA-256 direkomendasikan untuk keamanan jangka panjang.
- Digital signature memberikan tingkat keamanan yang tinggi untuk dokumen dan komunikasi digital.

5. Kesimpulan

Tugas ini menunjukkan bahwa algoritma modern memiliki peran penting dalam menjaga kerahasiaan, otentikasi, dan integritas data. Implementasi nyata membantu memahami cara kerja dan batasan dari masing-masing algoritma.

6. Lampiran






PS C:\Users\lenovo\Downloads\Kripto\TugasBesar2> c:; cd 'c:\Users\lenovo\Downloads\Kripto\TugasBesar2'; & 'c:\Python312\
thon.exe' 'c:\Users\lenovo\.vscode\extensions\ms-python.debugpy-2025.14.1-win32-x64\bundled\libs\debugpy\launcher' '52210
'--' 'C:\Users\lenovo\Downloads\Kripto\TugasBesar2\Hash Functions.py'
MD5: c0da827ce859899af708b64952723af5
SHA-1: c17a4135a824f8e6e6866fe35caba4d1ef4acff9
SHA-256: d418ae10b7fe4359f477aa9f1def512716a7af5878eec090584dd607c1791ff5
PS C:\Users\lenovo\Downloads\Kripto\TugasBesar2> ^C
PS C:\Users\lenovo\Downloads\Kripto\TugasBesar2> c:; cd 'c:\Users\lenovo\Downloads\Kripto\TugasBesar2'; & 'c:\Python312\
thon.exe' 'c:\Users\lenovo\.vscode\extensions\ms-python.debugpy-2025.14.1-win32-x64\bundled\libs\debugpy\launcher' '55702
'--' 'C:\Users\lenovo\Downloads\Kripto\TugasBesar2\Digital Signature.py'
Signature: UvnEn2ioG7XAijF3V9F2z2TmXUUXohj62+QdphsunJtvtnFEF36w+ruLDxmpYHh4LWhXLMTYRY5y15nrEIrQLLUJ6//scXLzVDOpEvHefirnXf
13pfdO++4LqwLfLKE+WfuS6NYwpxZoZHt4KptEBt4tTonJY5YFvrpmss65xJpz+fntFsMlem1dHrxeYFI/S8dF2+t0TIIli3CoIvqDKRIO0zG3/+5UGLfAX0g
aNyoUzjtj14LZvqFmdZyQomkRNwGf7eud4dAb3lMBZmCSmvMKJ3exMk4n041s288lMPZzXDfPnErki5TLULRP8MQ1Ec5+f+vT6uB8vbSfuQ==
Valid: True
PS C:\Users\lenovo\Downloads\Kripto\TugasBesar2> c:; cd 'c:\Users\lenovo\Downloads\Kripto\TugasBesar2'; & 'c:\Python312\
thon.exe' 'c:\Users\lenovo\.vscode\extensions\ms-python.debugpy-2025.14.1-win32-x64\bundled\libs\debugpy\launcher' '52609
'--' 'C:\Users\lenovo\Downloads\Kripto\TugasBesar2\Digital Signature.py'
Signature : rzoUaw/wVZt9NlD3l8hknyb9TsyGI1/Fa6wIcoQ1cwtia5ZvAX9dLBjT8H48NVy+GittRtt5LUessz+iWuVbMVgF8TLiTrn5dGR6SZ1Djqr/4
AFV/XkYOIhisotXVPHvZZS3fXe9yLzwfFJ4nZwL41go7OkqdxAW7exrheis1kE5FZ2le9J+7OdECp079VK4cf6XJ42WnheGpjIfD2NRI3SGbJ3kXnEWoKudg2
j80cq1Tc94v0q3DQE6PVC/rqeLMCTq8PbRmGMLi0sXejPx5GYPYNKj+vDrrrgVo6Lgwk5YE6f33vVY10M5wqA6v2gUT7kVgFvHFfPAtWzY4A==
Valid? : True