
1️⃣ Do we use RSA for encryption and decryption? Give example.

✔ **YES — RSA is used for both encryption and decryption.**

RSA uses **two different keys**:

Operation	Key Used
Encryption	Public Key (e, n)
Decryption	Private Key (d, n)

Simple Example

Let:

- Public key = (e = 7, n = 143)
- Private key = (d = 103, n = 143)
- Message = **9**

Encryption:

$$C = 9^7 \mod 143 = 48$$

Decryption:

$$M = 48^{103} \mod 143 = 9$$

✔ Original message recovered
✔ RSA used for both operations

2️⃣ AES vs RSA: Which has lower compute cost? Which is better?

✔ **AES is MUCH faster than RSA.**

👉 **AES (symmetric encryption)**

- Operates on **128-bit blocks**
- Extremely fast
- Used for encrypting large data
- Hardware acceleration available

👉 RSA (asymmetric encryption)

- Very slow (uses huge numbers like 1024/2048/4096 bits)
- Not suitable for encrypting big data
- Used only for:
    - Key exchange
    - Digital signatures
    - Encrypting small values like AES keys

Conclusion:

Algorithm	Speed	Use
AES	**Fast**	Large data encryption
RSA	**Slow**	Key exchange + signatures

✔ AES is better for performance
✖ RSA is too slow for bulk encryption

---

3 In industry and widespread use, which is used?

✔ Both are used together (hybrid cryptography)

This is how HTTPS, VPN, banking, and security systems work:

RSA is used for:

- Public key authentication
- Exchanging AES keys
- Digital signatures (SSL certificates)

AES is used for:

- Encrypting all data after the connection is secure
- Website traffic

- VPN data
- File encryption
- Hard disk encryption

Final Industry Answer

Task	Algorithm Used
Secure key exchange	**RSA**
Bulk data encryption	**AES**
Digital signatures	**RSA**
Internet security (HTTPS)	**RSA + AES**

✔ Final Short Answers (for exams)

Q1: Do we use RSA for encryption and decryption?

Yes. RSA encrypts with the **public key** and decrypts with the **private key**.
Example: If public key = (7, 143), message = 9 → ciphertext = 48.
Decrypt using private key = (103, 143) → get 9.

Q2: AES vs RSA compute cost — which is better?

AES is **far faster and cheaper** computationally.
RSA is slower because it uses huge integers (1024–4096 bits).

Q3: Which is used in industry?

Both are used together.
RSA for **key exchange / authentication**,
AES for **actual data encryption**.