Cryptographic Algorithm Analysis and Comparison Using CyberChef

Introduction

This project explores different cryptographic algorithms using CyberChef, analyzing their strengths, weaknesses, and practical applications. The algorithms chosen for evaluation include AES (symmetric encryption), RSA (asymmetric encryption), and SHA256 (hash function).

Selected Algorithms

1. Symmetric Encryption: AES (Advanced Encryption Standard) 2.

Asymmetric Encryption: RSA (Rivest-Shamir-Adleman)

3. Hashing Algorithm: SHA256 (Secure Hash Algorithm 256-bit)

Encryption and Decryption Using CyberChef

1. AES Encryption and Decryption

- Plaintext: "CyberSecurity is essential."
- Key: "MySecretKey12345"
- Mode: CBC (Cipher Block Chaining)
- Ciphertext Output: Base64 encoded encrypted text
- Decryption Process: Successfully retrieved original plaintext from ciphertext using the same keyand mode.

2. RSA Encryption and Decryption

- Plaintext: "Confidential Information"
- Key Size: 2048-bit

- Encryption Process: Public key used to encrypt the plaintext.

- Decryption Process: Private key successfully recovered the original plaintext.

3. Hashing Using SHA256

- Plaintext: "CyberSecurity2025"

- Hash Output: 64-character hexadecimal SHA256 hash.

- Observation: Hashing is a one-way function, making it irreversible.

Analysis and Comparison

Algorithm	Key Length	Security Level	Speed	Use Cases
AES	128/192/256-bit	High	Fast	Secure file encryption, communication security
RSA	1024/2048/4096-bit	Very High	Slow	Secure key exchange, digital signatures
SHA256	256-bit	Very High	Fast	Password hashing, data integrity checks

Cracking Sample Hashes

1. **MD5 Hash (801338b11e9d13070dc726cbc67ab160)**

    - Used an online hash cracking tool.

    - Possible password: "f!r5t"

2. **SHA256 Hash (5f22db794e7a7c5219980eb2a492f577804179e30be20c3db28623ed63f19c90)**

    - Possible password: “ I gave up after a hour “

Conclusion

- AES is efficient for encrypting large amounts of data but requires secure key management.
- RSA ensures high security but is computationally expensive, making it ideal for key exchange rather than bulk encryption.
- SHA256 is highly secure for password hashing but cannot be reversed.
- MD5 is weak and should not be used for security purposes.
- bcrypt provides strong password security due to built-in salting.

Final Thoughts

Understanding different cryptographic algorithms is crucial for cybersecurity. CyberChef provides an accessible way to experiment with encryption, decryption, and hashing techniques. For secure systems, a combination of AES, RSA, and SHA256 is recommended to balance efficiency and security.