# ALGORITHM VULNERABILITY ASSESSMENT

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithm type | Algorithms | Vulnerability in post quantum era | Justification |
| symmetric algorithm | Advanced Encryption Standard(AES) | None | Quantum computer on Grover’s algorithm with clock rate of 2THz would take a million years to break AES-128 (JimakosJimakos, 2024). |
|  | Twofish | None | Safer as it supports only 256 bit and not vulnerable to bruteforce. |
|  | Serpent | None | High security margin only second to AES. |
|  | Data Encrption Standard (DES) | None, Outdated | Uses 56-bit key (Grabbe, 2022). |
|  | Blowfish | None | Can take upto 448 bits. |
|  | Secure Hashing algorithm (SHA) | None | Uses 256 bits hashing algorithm against collision vulnerabilities and brute force attacks (Harish, 2024). |
| Asymmetric algorithm | Rivest Shamir Adleman (RSA) | Vulnerable | Succeptable to big enough quantum computer that uses qubits. |
|  | Elliptic Curve Cryptography (ECDSA, ECDH) | Vulnerable | Quantum computers can solve ECDLP efficiently (ExperiMENTAL, 2024). |
|  | Finite Field Cryptography (DSA) | Vulnerable | Quantum computational ability can crack it in days if not hours. |

# References

JimakosJimakos                      75511 gold badge55 silver badges1111 bronze badges, Daniel SDaniel S                      24.7k11 gold badge2929 silver badges6767 bronze badges and PrinceofmillerovoPrinceofmillerovo                      1522 bronze badges (2024) *Is AES-128 quantum safe?*, *Cryptography Stack Exchange*. Available at: https://crypto.stackexchange.com/questions/102671/is-aes-128-quantum-safe (Accessed: 26 August 2024).

Grabbe, J.O. (2022) *The des algorithm illustrated*, *The DES algorithm Illustrated*. Available at: https://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm (Accessed: 25 August 2024).

Harish, A. (2024) *2024 complete guide to sha encryption types*, *SecureW2*. Available at: https://www.securew2.com/blog/what-is-sha-encryption-sha-256-vs-sha-1#:~:text=SHA%2D256%20is%20secure%20due,a%20more%20secure%20hashing%20algorithm. (Accessed: 26 August 2024).

ExperiMENTAL (2024) *Does quantum computing spell the end for elliptic curve cryptography? not quite!*, *Medium*. Available at: https://medium.com/@jamie.brian.gilchrist/does-quantum-computing-spell-the-end-for-elliptic-curve-cryptography-not-quite-6f22ee202851#:~:text=The%20Quantum%20Threat%20to%20ECC&text=These%20advanced%20machines%2C%20armed%20with,Curve%20isn’t%20sufficient%20anymore. (Accessed: 26 August 2024).