The NSA retires RSA and keeps AES-256

No machine capable of either attack exists today. The same NSA advisory that retires RSA for national security systems keeps AES-256 as its required cipher.

BREAKS COMPLETELY

Public-key cryptography

RSA

Agreeing a secret key over an open line, and signing the certificate that proves a server's identity

Diffie-Hellman

Agreeing a secret key over an open line

Elliptic curve (ECDH, ECDSA)

The same 2 jobs, on smaller keys

Shor's method, published in 1994, recovers the private key directly from the public key. Larger keys do not help.

SURVIVES WITH A LARGER SIZE

Symmetric encryption and hashing

AES-256

Scrambling the actual content of a message or file

SHA-256

Storing proof of a password without the password

Grover's method halves effective strength, and NIST states that "doubling the key size will be sufficient." AES-128 is the exception.

Source: NIST IR 8105 (2016); NSA CNSA 2.0 FAQ. LaMarr Labs, lamarrlabs.com/resources