Which of the following types of encryption is classified as symmetric key cryptography?

ECC

RSA

AES

PGP

Answer: C

Explanation: The Advanced Encryption Standard (AES) was designed as a replacement for the Data Encryption Standard (DES). Both AES and DES are classified as symmetric key cryptography because their algorithms utilize the same key to encrypt and decrypt the data.

-=-=-=-

John is comparing two files that have the exact same MD5 hash, but the file contents are not identical. John doesn’t understand how this could occur since he believes that an MD5 hash is considered a truly unique fingerprint for a file and no two files could have the same MD5 hash. How do you explain this occurrence to John?

Man-in-the-Middle attack was performed

Brute-force attack was performed

Birthday attack was performed

XSS attack was performed

Answer: C

Explanation: Since an MD5 hash can only contain 128-bits to represent every possible input it receives, there are some collisions that may occur. This is known as a birthday attack because two hashes have the same value even though they have different inputs. These are not common, but they do occur due to the limited hash value size in MD5. Because of this, MD5 is being replaced with SHA-1 and SHA-256 in most applications.

-=-=-=-

Which of the following algorithms is categorized as asymmetric key cryptography?

Twofish

3DES

RC4

Diffie-Hellman

Answer: D

Explanation: Diffie-Hellman is an asymmetric algorithm used to exchange a shared secret key over an unprotected communications channel. This was first invented in the 1970s and can be used by IPSec and the TLS protocol to establish a shared secret key between two previously unknown devices.