

**WGU C839 OBJECTIVE ASSESSMENT 2 LATEST
VERSIONS (VERSION A & B) 2023-2024 /WGU
C839 INTRODUCTION TO CRYPTOGRAPHY OA
ACTUAL EXAM 350 QUESTIONS AND CORRECT
DETAILED ANSWERS WITH
RATIONALS|ALREADY GRADED A+**

WGU C839 OBJECTIVE ASSESSMENT VERSION A

Which of the following is NOT required for a hash?

A Minimum key length of 256 bits

B Variable-length input, fixed-length output

C Non-reversible

D Few collisions - ANSWER- A

learnexams

A _____ refers to a situation where two different inputs yield the same output.

A Substitution

B Convergence

C Collision

D Transposition - ANSWER- C

What is a salt?

A Key rotation

B Random bits intermixed with a hash to increase randomness and reduce collisions.

C Random bits intermixed with a symmetric cipher to increase randomness and make it more secure.

D Key whitening - ANSWER- B

RFC 1321 describes what hash?

A RIPEMD

B SHA1

C GOST

D MD5 - ANSWER- D

learnexams

What size block does FORK256 use?

A 256

B 128

C 512

D 64 - ANSWER- C

In 1977 researchers at MIT described what asymmetric algorithm?

A RSA

B AES

C DH

D EC - ANSWER- A

What is the formula $(M^e) \% n$ related to?

A Encrypting with EC

B Generating Mersenne primes

C Decrypting with RSA

D Encrypting with RSA - ANSWER- C

Which of the following equations is related to EC?

learnexams

A $P = Cd \% n$

B $Me \% n$

C $y^2 = x^3 + Ax + B$

D Let $m = (p-1)(q-1)$ - ANSWER- C

U.S. Patent 5,231,668 and FIPS 186 define what algorithm?

A AES

B RSA

C Elliptic Curve (EC)

D Digital Signature Algorithm (DSA) - ANSWER- D

What is X.509?

- A The standard for PGP certificates
- B The standard for encrypting email
- C The standard for FIPS 186

D The standard for digital certificates - ANSWER- D

What is contained in a CRL?

- A Keys for RSA
- B New certificates
- C Revoked certificates**
- D Keys for AES - ANSWER- C

learnexams

What does the Online Certificate Status Protocol (OCSP) provide?

- A Revoked certificates**
- B Hashing
- C VPN connectivity
- D Encryption - ANSWER- A

In terms of cryptanalysis, what does it mean to break a cipher?