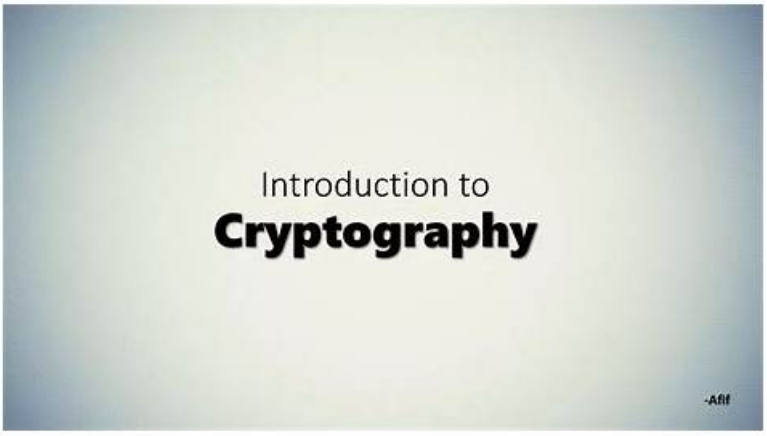
Introduction-to-Cryptography Fragen&Antworten - Introduction-to-Cryptography Examengine



PrüfungFrage hat ein professionelles IT-Team, das sich mit der Forschung der Fragen und Antworten zur WGU Introduction-to-Cryptography Zertifizierungsprüfung beschäftigt und Ihnen sehr effektive Prüfungsunterlagen und Online-Dienste bietet. Wenn Sie PrüfungFrage Produkte kaufen, wird PrüfungFrage Ihnen mit den neulich aktualisierten, sehr detaillierten Schulungsunterlagen von bester Qualität und genaue Prüfungsfragen und Antworten zur Verfügung stellen. So können Sie sich ganz unbesorgt auf Ihre WGU Introduction-to-Cryptography Zertifizierungsprüfung vorbereiten. Benutzen Sie ganz beruhigt unsere PrüfungFrage Produkte. Sie können 100% die Introduction-to-Cryptography Prüfung erfolgreich ablegen.

Je früher die Zertifizierung der WGU Introduction-to-Cryptography zu erwerben, desto hilfreicher ist es für Ihre Karriere in der IT-Branche. Vielleicht haben Sie erfahren, dass die Vorbereitung dieser Prüfung viel Zeit oder Gebühren fürs Training braucht. Aber die WGU Introduction-to-Cryptography Prüfungssoftware von uns widerspricht diese Darstellung. Die komplizierte Sammlung und Ordnung der Prüfungsunterlagen der WGU Introduction-to-Cryptography werden von unserer professionellen Gruppen fertiggemacht. Genießen Sie doch die wunderbare Wirkungen der Prüfungsvorbereitung und den Erfolg bei der WGU Introduction-to-Cryptography Prüfung!

>> Introduction-to-Cryptography Fragen&Antworten <<

Introduction-to-Cryptography Examengine & Introduction-to-Cryptography Online Test

Viele Webseiten bieten WGU Introduction-to-Cryptography Zertifizierungsunterlagen und andere Unterlagen. Aber wir PrüfungFrage sind die einzige Website, die besten WGU Introduction-to-Cryptography Zertifizierungsunterlagen zu bieten. Mit der Hilfe von PrüfungFrage können Sie nur einmal WGU Introduction-to-Cryptography Zertifizierungsprüfung zu bestehen. Die WGU Introduction-to-Cryptography Prüfungsfragen und Testantworten von PrüfungFrage sind von reichen Erfahrungen und Kenntnissen gesammelt. Diese bieten Ihnen eine gute Chance, in IT-Industrie zu entwickeln.

WGU Introduction to Cryptography HNO1 Introduction-to-Cryptography Prüfungsfragen mit Lösungen (Q39-Q44):

39. Frage
(A security analyst uses a polyalphabetic substitution cipher with a keyword of YELLOW to encrypt a message. Which cipher should be used to encrypt the message?)

- A. Caesar
- B. Vigenere
- C. Playfair
- D. Pigpen

Antwort: B

Begründung:

A polyalphabetic substitution cipher uses multiple substitution alphabets rather than a single fixed mapping. The classic cipher that uses a keyword to select shifting alphabets across the message is the Vigenere cipher. In Vigenere, each plaintext letter is shifted by an amount determined by the corresponding key letter (repeating the keyword as needed). For example, a keyword like "YELLOW" is aligned under the plaintext; each key character defines a Caesar shift (A=0, B=1, ...) applied to the plaintext character, producing ciphertext. This rotation of alphabets across positions makes Vigenere more resistant to simple frequency analysis than monoalphabetic substitution, because the same plaintext letter may encrypt to different ciphertext letters depending on its position relative to the key.
The Pigpen cipher is a symbol substitution cipher, Caesar is monoalphabetic with a single shift, and Playfair is a digraph substitution cipher using a 5×5 key square, not the repeating-key polyalphabetic method described. Therefore, the correct cipher is Vigenere.

40. Frage
(Which authentication method allows a customer to authenticate to a web service?)

- A. One-way server authentication
- B. Mutual authentication
- C. End-to-end authentication
- D. One-way client authentication

Antwort: D

Begründung:
One-way client authentication is the method where the client (customer) proves its identity to the server (web service). In cryptographic terms, this is commonly implemented through client credentials such as client TLS certificates (mTLS from the server's perspective) or through authentication protocols layered over TLS (for example, signed tokens), but the defining direction is that the client is the party being authenticated. In a strict TLS certificate-authentication framing, client authentication occurs when the server requests a client certificate during the handshake and the client demonstrates possession of the corresponding private key (via signature in handshake messages). The server then validates the client certificate chain and authorization policy. One-way server authentication, by contrast, authenticates only the server to the client and does not identify the customer. Mutual authentication authenticates both sides simultaneously; while it includes client authentication, it is broader than what the question asks. "End-to-end authentication" describes assurance between endpoints across intermediaries, but it is not the specific "customer authenticates to service" method in certificate-based terminology. Therefore, the best answer is one-way client authentication.

41. Frage
(What is the value of 51 mod 11?)

- A. 05
- B. 04
- C. 0
- D. 07

Antwort: D

Begründung:
The value 51 mod 11 is the remainder after dividing 51 by 11. Modular arithmetic is widely used in cryptography to keep computations within a finite set of residues, such as in RSA where values are taken modulo n, or in Diffie-Hellman where exponents and group elements are reduced modulo a prime. To compute 51 mod 11, find the largest multiple of 11 less than or equal to 51. Multiples of 11 are 11, 22, 33, 44, 55. The closest without exceeding 51 is 44. Subtracting gives 51 # 44 = 7, so the remainder is 7. Therefore, 51 mod 11 = 7, matching option "07." This remainder is always in the range
0 through 10 because the modulus is 11. Such residue computations underpin the "wraparound" behavior that makes modular exponentiation and inverse computations well-defined in cryptographic groups.

42. Frage
(Which type of exploit involves looking for different inputs that generate the same hash?)

- A. Algebraic attack
- B. Birthday attack
- C. Differential cryptanalysis

- D. Linear cryptanalysis

Antwort: B

Begründung:
A birthday attack targets hash functions by exploiting the birthday paradox: collisions (two different inputs producing the same hash output) can be found much faster than brute-forcing a specific preimage. For an n-bit hash, the expected work to findanycollision is on the order of 2