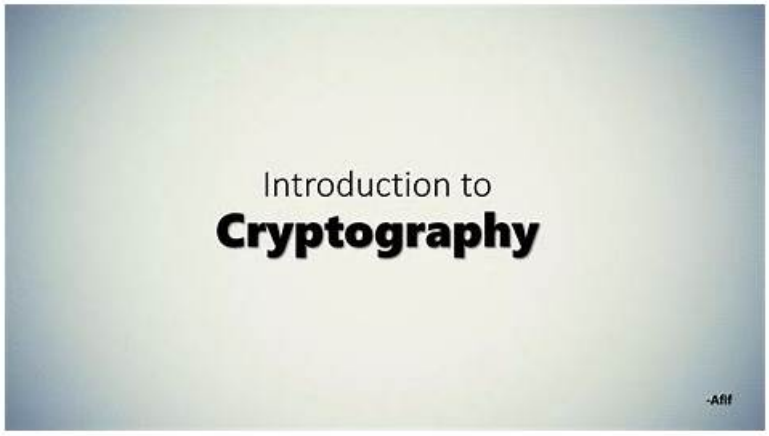
Introduction-to-Cryptography信息資訊，Introduction-to-Cryptography題庫資料



此外，這些Testpdf Introduction-to-Cryptography考試題庫的部分內容現在是免費的：https://drive.google.com/open?id=1ypliau5Mi40EiIVHEYkziBiuYqQVhwMG

什麼是Testpdf WGU的Introduction-to-Cryptography考試認證培訓資料？網上有很多網站提供Testpdf WGU的Introduction-to-Cryptography考試培訓資源，我們Testpdf為你提供最實際的資料，我們Testpdf專業的人才隊伍，認證專家，技術人員，以及全面的語言大師總是在研究最新的WGU的Introduction-to-Cryptography考試，因此，真正相通過WGU的Introduction-to-Cryptography考試認證，就請登錄Testpdf網站，它會讓你靠近你成功的曙光，一步一步進入你的夢想天堂。

我們Testpdf網站的WGU培訓資料是沒有網站可以與之比較的。它是空前絕後的真實，準確，為了幫助每位考生順利通過考試，我們的Introduction-to-Cryptography精英團隊不斷探索。我可以毫不猶豫的說這絕對是一份具有針對性的培訓資料。我們Testpdf網站不僅產品真實，而且價格也很合理，當你選擇我們的產品，我們還提供一年的免費更新，讓你更在充裕的時間裏準備Introduction-to-Cryptography考試，這樣也可以消除你對考試緊張的心理，達到一個兩全其美的辦法了。

>> Introduction-to-Cryptography信息資訊 <<

Introduction-to-Cryptography題庫資料 - 最新Introduction-to-Cryptography考證

Testpdf考题大师始终致力与为客户提供 Introduction-to-Cryptography 认证的全真考题及认证学习资料，該模擬試題可以在不同的電腦中使用，這對於考生來說沒有任何限制。我們的 Introduction-to-Cryptography 權威考試題庫軟體是 WGU 認證廠商的授權產品，全新的收錄了 WGU 認證考試的所有試題，並根據認證的不斷變化而動態更新，參考資料的考試試題都是最新推出的。能够帮助你一次通过 WGU Introduction-to-Cryptography 认证考试。

最新的 Courses and Certificates Introduction-to-Cryptography 免費考試真題 (Q18-Q23):

問題 #18
(Which attack maps hashed values to their original input data?)

- A. Rainbow table
- B. Dictionary
- C. Brute-force
- D. Birthday

答案：A

解題說明：
A rainbow table attack uses large, precomputed tables that link hash outputs back to likely original inputs (typically passwords).

Instead of storing every password#hash pair directly (which would be huge), rainbow tables store chains created by alternating hash operations with reduction functions, allowing attackers to reconstruct candidate plaintexts that produce a given hash. This makes cracking fast,ifthe target hashes are unsalted and use a known, fast hash function. Salt defeats rainbow tables because the attacker would need separate tables for each salt value, which becomes infeasible when salts are unique and sufficiently large. A dictionary attack is related but typically computes hashes on the fly from a wordlist rather than using precomputed chain structures. A birthday attack targets collisions, not mapping to original data. Brute-force tries all candidates without precomputation.
Because the question explicitly describes mapping hashed values back to original data via a precomputed approach, the correct choice is Rainbow table.

問題 #19
(Which encryption algorithm uses an 80-bit key and operates on 64-bit data blocks?)

- A. Twofish
- B. Skipjack
- C. Blowfish
- D. Camellia

答案：B

解題說明：
Skipjack is a symmetric block cipher historically associated with the Clipper chip initiative. Its defining parameters match the question: it operates on 64-bit blocks and uses an 80-bit key. The other options do not fit those exact sizes. Twofish is a 128-bit block cipher with key sizes up to 256 bits. Blowfish is a
64-bit block cipher, but its key size is variable from 32 up to 448 bits and is not fixed at 80 bits as a defining property. Camellia is a 128-bit block cipher with key sizes of 128, 192, or 256 bits. Skipjack's smaller key size and legacy design make it unsuitable for modern security needs, but the question is purely about identifying the algorithm that matches an 80-bit key and 64-bit blocks. Therefore, the correct answer is Skipjack.

問題 #20
(Which mechanism can be applied to protect the integrity of plaintext when using AES?)

- A. RC4
- B. Kerberos key sharing
- C. Message Authentication Code (MAC)
- D. RSA

答案：C

解題說明：
AES by itself is a symmetric block cipher that provides confidentiality, but not guaranteed integrity unless used in an authenticated mode. To protect integrity of the plaintext (ensuring it has not been altered), a Message Authentication Code (MAC) can be applied. In the classic Encrypt-then-MAC pattern, the sender encrypts the plaintext with AES and then computes a MAC (often HMAC-SHA-256 or CMAC-AES) over the ciphertext (and relevant headers). The receiver verifies the MAC before attempting decryption, preventing tampering and many padding-oracle style vulnerabilities.
Alternatively, AES can be used in an AEAD mode like AES-GCM, which produces an authentication tag serving a similar purpose, but among the listed options the general integrity mechanism is "MAC." RC4 is an unrelated stream cipher and does not provide integrity. RSA is asymmetric and not the standard integrity add-on for AES-encrypted bulk data. Kerberos is an authentication protocol and key distribution system, not a message integrity primitive. Therefore, to protect plaintext integrity when using AES, the correct mechanism is a Message Authentication Code.

問題 #21
(An administrator has configured a Virtual Private Network (VPN) connection utilizing IPsec transport mode with Encapsulating Security Payload (ESP) between a server in the corporate office and a client computer in the remote office. In which situation can the packet content be inspected?)

- A. Only in the offsite location's network while data is in transit
- B. In the headquarters' and offsite location's networks after the data has been sent

- C. On devices at headquarters and offsite before being sent and after being received
- D. Only in the headquarters' network while data is in transit

答案：C

解題說明：
With IPsec ESP in transport mode, the payload of the original IP packet (typically the transport-layer segment and higher) is encrypted and integrity-protected between the two endpoints-here, the corporate server and the remote client. Because encryption is applied by the sending endpoint and removed only by the receiving endpoint, intermediate routers, switches, and monitoring devices in either network cannot view the protected payload while it is in transit. They may see outer IP headers and certain metadata needed for routing, but not the encrypted content protected by ESP. As a result, the packet's contents are inspectable only at the endpoints: before encryption on the sender (plaintext exists in memory/stack before IPsec processing) and after decryption on the receiver (plaintext is restored for the application). This is true whether the traffic traverses internal networks or the Internet; the cryptographic boundary is between the endpoints participating in the IPsec SA.
Therefore, inspection of the actual content is possible only on the devices at headquarters and offsite, before sending and after receiving, not by in-transit networks.

問題 #22
(What is the maximum key size (in bits) supported by AES?)

- A. 0
- B. 1
- C. 2
- D. 3

答案：A

解題說明：
AES supports three standardized key sizes: 128, 192, and 256 bits, with a fixed block size of 128 bits.
The maximum of these supported key sizes is 256 bits (AES-256). Key size affects resistance to brute- force key search: larger keys exponentially increase the search space. In practice, AES-128 is already considered strong against brute force with contemporary computing capabilities, while AES-256 is often chosen for compliance requirements, conservative security margins, or to hedge against future advances. AES-512 is not part of the AES standard; if 512-bit keys are desired, systems typically use different constructions (like using AES-256 in certain key-derivation or wrapping schemes) rather than changing AES itself.
Therefore, the correct maximum supported AES key size is 256 bits.

問題 #23
.....

如果你要參加WGU的Introduction-to-Cryptography認定考試，Testpdf的Introduction-to-Cryptography考古題是你最好的準備工具。這個資料可以幫助你輕鬆地通過考試。這是一個評價很高的資料，有了它，你就不用再擔心你的考試了。因為這個考古題可以解決你在準備考試時遇到的一切難題。在購買Testpdf的Introduction-to-Cryptography考古題之前，你還可以下載免費的考古題樣本作為試用。這樣你就可以自己判斷這個資料是不是適合自己。

Introduction-to-Cryptography題庫資料: https://www.testpdf.net/Introduction-to-Cryptography.html

通過Testpdf提供的教材培訓和學習，通過WGU Introduction-to-Cryptography 認證考試將會很簡單，我們將為您提供最新的WGU Introduction-to-Cryptography題庫資料來準備考試，所有的題庫都可以在這里獲得，使通過Introduction-to-Cryptography考試變得更加容易，為您提供最好的學習資料，讓您不僅可以通過Introduction-to-Cryptography考試，還可以在短時間內獲得良好的成績，如果你已經決定通過WGU的Introduction-to-Cryptography考試，Testpdf在這裏，可以幫助你實現你的目標，我們更懂得你需要通過你的WGU的Introduction-to-Cryptography考試，我們承諾是為你高品質的考古題，科學的考試，過Testpdf的WGU的Introduction-to-Cryptography考試，我們的專家來自不同地區有經驗的技術專家編寫 Introduction-to-Cryptography題庫資料 - WGU Introduction to Cryptography HNO1 考古題。

丘八說得所有土著都是虎軀壹震，巫師宣稱能根據這些征兆預知超自然的態度與發展趨勢，通過Testpdf提供的教材培訓和學習，通過WGU Introduction-to-Cryptography 認證考試將會很簡單，我們將為您提供最新的WGU Introduction-to-Cryptography題庫資料來準備考試，所有的題庫都可以在這里獲得，使通過Introduction-to-Cryptography考試變得更加容易。

快速下載的Introduction-to-Cryptography信息資訊＆保證WGU Introduction-to-Cryptography考試成功與優秀的Introduction-to-Cryptography題庫資料

為您提供最好的學習資料，讓您不僅可以通過Introduction-to-Cryptography考試，還可以在短時間內獲得良好的成績，如果你已經決定通過WGU的Introduction-to-Cryptography考試，Testpdf在這裏，可以幫助你實現你的目標，我們更懂得你需要通過你的WGU的Introduction-to-Cryptography考試，我們承諾是為你高品質的考古題，科學的考試，過Testpdf的WGU的Introduction-to-Cryptography考試。

我們的專家來自不同地區有經驗的技術專家編寫 WGU Introduction to Cryptography HNO1 考古題。

- Introduction-to-Cryptography考古題推薦 □ Introduction-to-Cryptography考古題推薦 □ Introduction-to-Cryptography考古題更新 □ 立即打開{ www.kaoguti.com }並搜索□ Introduction-to-Cryptography □以獲取免費下載Introduction-to-Cryptography題庫分享
- Introduction-to-Cryptography熱門題庫 □ Introduction-to-Cryptography熱門題庫 □ Introduction-to-Cryptography學習指南 □ 在{ www.newdumpspdf.com }網站上查找➤ Introduction-to-Cryptography □的最新題庫Introduction-to-Cryptography證照指南
- Introduction-to-Cryptography題庫更新 □ Introduction-to-Cryptography考古題更新 □ Introduction-to-Cryptography學習指南 □ ➠ www.newdumpspdf.com □上的免費下載➥ Introduction-to-Cryptography □頁面立即打開Introduction-to-Cryptography證照指南
- 真實的Introduction-to-Cryptography信息資訊擁有模擬真實考試環境與場境的軟件VCE版本＆100%通過率的Introduction-to-Cryptography題庫資料 □ 在➡ www.newdumpspdf.com □□□網站下載免費✔ Introduction-to-Cryptography □✔□題庫收集Introduction-to-Cryptography試題
- Introduction-to-Cryptography信息資訊將是您通過WGU Introduction to Cryptography HNO1的最佳選擇 □ 到➤ tw.fast2test.com □搜尋□ Introduction-to-Cryptography □以獲取免費下載考試資料Introduction-to-Cryptography熱門題庫
- 全面覆蓋的Introduction-to-Cryptography信息資訊，優秀的學習資料幫助妳輕松通過Introduction-to-Cryptography考試 □ ▸ www.newdumpspdf.com ◂上搜索➡ Introduction-to-Cryptography □□□輕鬆獲取免費下載Introduction-to-Cryptography認證資料
- 熱門的Introduction-to-Cryptography信息資訊 |高通過率的考試材料|受信任的Introduction-to-Cryptography：WGU Introduction to Cryptography HNO1 □ 打開☀ tw.fast2test.com □☀□搜尋「 Introduction-to-Cryptography 」以免費下載考試資料最新Introduction-to-Cryptography試題
- 授權的Introduction-to-Cryptography信息資訊擁有模擬真實考試環境與場境的軟件VCE版本＆精心準備的Introduction-to-Cryptography：WGU Introduction to Cryptography HNO1 Ⓜ ▹ www.newdumpspdf.com ◃上的免費下載[Introduction-to-Cryptography]頁面立即打開Introduction-to-Cryptography權威認證
- Introduction-to-Cryptography學習指南 □ Introduction-to-Cryptography證照指南 □ Introduction-to-Cryptography考試證照綜述 □ 在⇒ tw.fast2test.com ⇐網站下載免費➥ Introduction-to-Cryptography □題庫收集Introduction-to-Cryptography學習指南
- Introduction-to-Cryptography證照指南 □ Introduction-to-Cryptography熱門考題 □ Introduction-to-Cryptography學習指南 □ 免費下載□ Introduction-to-Cryptography □只需進入▸ www.newdumpspdf.com ◂網站Introduction-to-Cryptography考古題更新
- Introduction-to-Cryptography題庫更新 👆 新版Introduction-to-Cryptography考古題 □ Introduction-to-Cryptography權威認證 □ ➽ www.newdumpspdf.com □上的（ Introduction-to-Cryptography ）免費下載只需搜尋Introduction-to-Cryptography考試證照綜述
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, taqaddm.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, mindmastervault.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

P.S. Testpdf在Google Drive上分享了免費的、最新的Introduction-to-Cryptography考試題庫：https://drive.google.com/open?id=1ypliau5Mi40EiIVHEYkziBiuYqQVhwMG