Ciphers Job Interview Questions And Answers

Interview Questions Answers

https://interviewquestionsanswers.org/

About Interview Questions Answers

Interview Questions Answers . ORG is an interview preparation guide of thousands of Job Interview Questions And Answers, Job Interviews are always stressful even for job seekers who have gone on countless interviews. The best way to reduce the stress is to be prepared for your job interview. Take the time to review the standard interview questions you will most likely be asked. These interview questions and answers on Ciphers will help you strengthen your technical skills, prepare for the interviews and quickly revise the concepts.

If you find any **question or answer** is incorrect or incomplete then you can **submit your question or answer** directly with out any registration or login at our website. You just need to visit Ciphers Interview Questions And Answers to add your answer click on the *Submit Your Answer* links on the website; with each question to post your answer, if you want to ask any question then you will have a link *Submit Your Question*; that's will add your question in Ciphers category. To ensure quality, each submission is checked by our team, before it becomes live. This Ciphers Interview preparation PDF was generated at **Wednesday 29th November, 2023**

You can follow us on FaceBook for latest Jobs, Updates and other interviews material.
www.facebook.com/InterviewQuestionsAnswers.Org

Follow us on Twitter for latest Jobs and interview preparation guides.
https://twitter.com/InterviewQA

If you need any further assistance or have queries regarding this document or its material or any of other inquiry, please do not hesitate to contact us.

Best Of Luck.

Interview Questions Answers.ORG Team
https://InterviewQuestionsAnswers.ORG/
Support@InterviewQuestionsAnswers.ORG

Ciphers Interview Questions And Answers Guide.

Question - 1:

What is IDEA?

Ans:

IDEA (International Data Encryption Algorithm) is the second version of a block cipher designed and presented by Lai and Massey. It is a 64-bit iterative block cipher with a 128-bit key and eight rounds. While the cipher is not Feistel, decryption is carried out in the same manner as encryption once the decryption subkeys have been calculated from the encryption subkeys. The cipher structure was designed to be easily implemented in both software and hardware, and the security of IDEA relies on the use of three incompatible types of arithmetic operations on 16-bit words. The speed of IDEA in software is similar to that of DES.

View All Answers

Question - 2:

What is the RC5?

Ans:

RC5 is a fast block cipher designed by Rivest for RSA Data Security. It is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. The block size can be 32, 64, or 128 bits long. The number of rounds can range from 0 to 255. The key can range from 0 bits to 2048 bits in size. Such built-in variability provides flexibility in levels of security and efficiency.
There are three routines in RC5: key expansion, encryption , and decryption. In the key-expansion routine, the user-provided secret key is expanded to fill a key table whose size depends on the number of rounds. The key table is then used in both encryption and decryption. The encryption routine consists of three primitive operations: addition, bitwise exclusive-or, and rotation. The exceptional simplicity of RC5 makes it easy to implement and analyze. Indeed, like RSA, RC5 can be written on the "back of the envelope" (except for key expansion).

View All Answers

Question - 3:

What is RC2?

Ans:

RC2 is a variable key-size block cipher designed by Rivest for RSA Data Security. "RC" stands for "Ron's Code" or "Rivest's Cipher." It is faster than DES and is designed as a "drop-in" replacement for DES. It can be made more secure or less secure than DES against exhaustive key search by using appropriate key sizes. It has a block size of 64 bits and is about two to three times faster than DES in software. The algorithm is confidential and proprietary to RSA Data Security. RC2 can be used in the same modes as DES.

View All Answers

Question - 4:

What are G-DES, DESX?

Ans:

G-DES was devised by Schaumuller-Bichl to improve on the performance of DES by defining a cipher based on DES with a larger block size, but without an increase in the amount of computation required. It was claimed that G-DES was as secure as DES since the cipher was based on DES. However, Biham and Shamir showed that G-DES with the recommended parameter sizes is easily broken and that any alterations of G-DES parameters that result in a cipher faster than DES are less secure than DES.

View All Answers

Question - 5:

How does One Use Triple-DES in CBC Mode?

Ans:

Until recently, the most significant use of triple-DES was for the encryption of single DES keys, and there was really no need to consider how one might implement various block cipher modes when the block cipher in question is actually one derived from multiple encryption. However, as DES nears the end of its useful lifetime, more thought is being given to an increasingly widespread use of triple-DES.

View All Answers

Question - 6:

What is Triple-DES?

Ans:

For some time it has been common practice to protect and tansport a key for DES encryption with triple-DES. This means that the plaintext is, in effect, encrypted three times. There are, of course. a variety of ways of doing this; we will explore these ways below. See Question 85 for a discussion of multiple encryption in general.
A number of modes of triple-encryption have been proposed:
DES-EEE3: Three DES encryptions with three different keys.
DES-EDE3: Three DES operations in the sequence encrypt-decrypt-encrypt with three different keys.
DES-EEE2 and DES-EDE2: Same the previrous formats except that the first and third operations use the same key.
Attacks on two-key triple-DES have been proposed by Merkle and Hellman [MH81] and Van Oorschot and Wiener [VW91], but the data requirements of these attacks make them impractical.

View All Answers

Question - 7:

What is DES with Independent Subkeys?

Ans:

The DES algorithm derives sixteen 48-bit subkeys, for use in each of the 16 rounds, from the 56-bit secret key supplied by the user. It is interesting to consider the effect of using a 768-bit key (divided into 16 48-bit subkeys) in place of the 16 related 48-bit keys that are generated by the key schedule in the DES algorithm.

View All Answers

Question - 8:

Is DES a Group?

Ans:

No, DES is not a group. This issue was settled only after many years of speculation and circumstantial evidence and this result seems to imply that techniques such as triple encryption do in fact increase the security of DES.

View All Answers

Question - 9:

What are the Alternatives to DES?

Ans:

Over the years, various new block cipher algorithms have been designed as alternatives to DES. One is FEAL, a cipher for which numerous attacks have been discovered. IDEA is a cipher designed by Lai and Massey that seems much more promising and two more recent designs are RC5 and SAFER. In addition, the U.S. government announced in 1993 an algorithm called Skipjack as part of its Capstone project. Skipjack operates on 64-bit blocks of data, as does DES, but uses 80-bit keys, as opposed to the 56-bit keys in DES. However, the details of Skipjack are classified, so Skipjack is only available in hardware from government-authorized manufacturers.

View All Answers

Question - 10:

Can DES be Exported from the United States?

Ans:

Export of DES, either in hardware or software, is strictly regulated by the U.S. State Department and the NSA. The government rarely approves export of DES, despite the fact that DES is widely available overseas; financial institutions and foreign subsidiaries of U.S. companies are exceptions.

View All Answers

Question - 11:

Should One Test for Weak Keys in DES?

Ans:

Since there are 256 possible DES keys the chance of picking a weak or semi-weak key at random is 2-52. As long as the user-provided key is chosen entirely at random, they can be safely ignored when DES is used for encryption. Despite this, some users prefer to test whether a key to be used for DES encryption is in fact a weak key. Such a test will have no significant impact on the time required for encryption.

View All Answers

Question - 12:

Has DES been Broken?

Ans:

No easy attack on DES has been discovered, despite the efforts of many researchers over many years. The obvious method of attack is brute-force exhaustive search of the key space; this takes 255 steps on average. Early on it was suggested that a rich and powerful enemy could build a special-purpose computer capable of breaking DES by exhaustive search in a reasonable amount of time. Later, Hellman [Hel80] showed a time-memory trade-off that allows improvement over exhaustive search if memory space is plentiful, after an exhaustive precomputation. These ideas fostered doubts about the security of DES. There were also accusations that the NSA had intentionally weakened DES. Despite these suspicions, no feasible way to break DES faster than exhaustive search was discovered. The cost of a specialized computer to perform exhaustive search (requiring 3.5 hours on average) has been estimated by Wiener at one million dollars.

View All Answers

Question - 13:

What is DES?

Ans:

DES is the Data Encryption Standard, an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard; the details can be found in the latest official FIPS (Federal Information Processing Standards) publication concerning DES. It was originally developed at IBM. DES has been extensively studied since its publication and is the most well-known and widely used cryptosystem in the world.
DES is a symmetric cryptosystem: when used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for single-user encryption, such as to store files on a hard disk in encrypted form. In a multi-user environment, secure key distribution may be difficult; public-key cryptography provides an ideal solution to this problem

View All Answers

Question - 14:

At What Point Does an Attack Become Practical?

Ans:

There is no easy answer to this question since it depends on many distinct factors. Not only must the work and computational resources required by the cryptanalyst be reasonable, but the amount and type of data required for the attack to be successful must also be taken into account.
One classification distinguishes among cryptanalytic attacks according to the data they require in the following way: chosen plaintext or chosen ciphertext, known plaintext, and ciphertext-only. (This classification is not particular to secret-key ciphers and can be applied to cryptanalytic attacks on any cryptographic function.)

View All Answers

Question - 15:

How Can Data Compression be Used With Encryption?

Ans:

Data compression removes redundant character strings in a file. This means that the compressed file has a more uniform distribution of characters. In addition to providing shorter plaintext and ciphertext, which reduces the amount of time needed to encrypt, decrypt and transmit a file, the reduced redundancy in the plaintext can potentially hinder certain cryptanalytic attacks.
By contrast, compressing a file after encryption is inefficient. The ciphertext produced by a good encryption algorithm should have an almost statistically uniform distribution of characters. As a consequence, a compression algorithm should be unable to find redundant patterns in such text and there will be little, if any, data compression. In fact, if a data compression algorithm is able to significantly compress encrypted text, then this indicates a high level of redundancy in the ciphertext which, in turn, is evidence of poor encryption.

View All Answers

Question - 16:

What are Algebraic Attacks?

Ans:

Algebraic attacks are a class of techniques which rely for their success on some block cipher exhibiting a high degree of mathematical structure.
For instance, it is conceivable that a block cipher might exhibit what is termed a group structure. If this were the case, then encrypting a plaintext under one key and then encrypting the result under another key would always be equivalent to single encryption under some other single key. If so, then the block cipher would be considerably weaker, and the use of multiple encryption would offer no additional security over single encryption. For most block ciphers, the question of whether they form a group is still open. For DES , however, it is known that the cipher is not a group.

View All Answers

Question - 17:

What is a Weak Key for a Block Cipher?

Ans:

Weak keys are secret keys with a certain value for which the block cipher in question will exhibit certain regularities in encryption or, in other cases, a poor level of encryption. For instance, with DES there are four keys for which encryption is exactly the same as decryption. This means that if one were to encrypt twice with one of these weak keys, then the original plaintext would be recovered. For IDEA there is a class of keys for which cryptanalysis is greatly facilitated and the key can be recovered. However, in both these cases, the number of weak keys is such a small fraction of all possible keys that the chance of picking one at random is exceptionally slight. In such cases, they pose no significant threat to the security of the block cipher when used for encryption.

View All Answers

Question - 18:

What is Linear Cryptanalysis?

Ans:

Linear cryptanalysis was first devised by Matsui and Yamagishi in an attack on FEAL. It was extended by Matsui to attack DES. Linear cryptanalysis is a known plaintext attack and uses a linear approximation to describe the behavior of the block cipher. Given sufficient pairs of plaintext and corresponding ciphertext, bits of information about the key can be obtained and increased amounts of data will usually give a higher probability of success.

View All Answers

Question - 19:

What is Differential Cryptanalysis?

Ans:

Differential cryptanalysis is a type of attack that can be mounted on iterative block ciphers. These techniques were first introduced by Murphy [Mur90] in an attack on FEAL-4, but they were later improved and perfected by Biham and Shamir who used them to attack DES. Differential cryptanalysis is basically a chosen plaintext attack and relies on an analysis of the evolution of the differences between two related plaintexts as they are encrypted under the same key. By careful analysis of the available data, probabilities can be assigned to each of the possible keys and eventually the most probable key is identified as the correct one.

View All Answers

Question - 20:

What is Exhaustive Key Search?

Ans:

Exhaustive key search, or brute-force search, is the basic technique of trying every possible key in turn until the correct key is identified. To identify the correct key it may be necessary to possess a plaintext and its corresponding ciphertext, or if the plaintext has some recognizable characteristic, ciphertext alone might suffice. Exhaustive key search can be mounted on any cipher and sometimes a weakness in the key schedule of the cipher can help improve the efficiency of an exhaustive key search attack.

Advances in technology and computing performance will always make exhaustive key search an increasingly practical attack against keys of a fixed length. When DES was designed, it was generally considered secure against exhaustive key search without a vast financial investment in hardware. Over the years, this line of attack will become increasingly attractive to a potential adversary.

View All Answers

Question - 21:

What is a Feistel Cipher?

Ans:

Feistel ciphers are a special class of iterated block ciphers where the ciphertext is calculated from the plaintext by repeated application of the same transformation or round function. Feistel ciphers are also sometimes called DES-like ciphers.
In a Feistel cipher, the text being encrypted is split into two halves. The round function f is applied to one half using a subkey and the output of f is exclusive-ored with the other half. The two halves are then swapped. Each round follows the same pattern except for the last round where there is no swap.

View All Answers

Question - 22:

What is an Iterated Block Cipher?

Ans:

An iterated block cipher is one that encrypts a plaintext block by a process that has several rounds. In each round, the same transformation or round function is applied to the data using a subkey. The set of subkeys are usually derived from the user-provided secret key by a key schedule.

View All Answers

Question - 23:

What is a Block Cipher?

Ans:

A block cipher transforms a fixed-length block of plaintext data into a block of ciphertext data of the same length. This transformation takes place under the action of a user-provided secret key. Decryption is performed by applying the reverse transformation to the ciphertext block using the same secret key. The fixed length is called the block size, and for many block ciphers, the block size is 64 bits.

View All Answers

Cryptography Most Popular & Related Interview Guides

1 : **Cryptography General Interview Questions and Answers.**

2 : Typesetter Interview Questions and Answers.

3 : Cryptography Teacher Interview Questions and Answers.

4 : Typewriter Interview Questions and Answers.

5 : Cryptography Interview Questions and Answers.

6 : Encryption Decryption Interview Questions and Answers.

7 : Digital Certificates Interview Questions and Answers.

8 : Cryptography Algorithm Interview Questions and Answers.

9 : Cryptography Protocols Interview Questions and Answers.

Follow us on FaceBook
www.facebook.com/InterviewQuestionsAnswers.Org

Follow us on Twitter
https://twitter.com/InterviewQA

For any inquiry please do not hesitate to contact us.

Interview Questions Answers.ORG Team
https://InterviewQuestionsAnswers.ORG/
support@InterviewQuestionsAnswers.ORG