# Digital Certificates 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 Digital Certificates 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 Digital Certificates 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 Digital Certificates category. To ensure quality, each submission is checked by our team, before it becomes live. This Digital Certificates 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**

# Digital Certificates Interview Questions And Answers Guide.

**Question - 1:**

What are Certificate Revocation Lists(CRLs)?

**Ans:**

A certificate revocation list (CRL) is a list of certificates that have been revoked before their scheduled expiration date. There are several reasons why a certificate might need to be revoked and placed on a CRL. For instance, the key specified in the certificate might have been compromised, or, the user specified in the certificate may no longer have authority to use the key. For example, suppose the user name associated with a key is "Alice Avery, Vice President, Argo Corp." If Alice were fired, her company would not want her to be able to sign messages with that key, and therefore, the company would place the certificate on a CRL.
When verifying a signature, one can check the relevant CRL to make sure the signer's certificate has not been revoked. Whether it is worth the time to perform this check depends on the importance of the signed document.

View All Answers

**Question - 2:**

What if a Certifying Authoritys Key is Lost or Compromised?

**Ans:**

If the certifying authority's key is lost or destroyed but not compromised, certificates signed with the old key are still valid, as long as the verifier knows to use the old public key to verify the certificate.
In some designs for certificate-signing devices, encrypted backup copies of the CA's private key are kept, so a CA that loses its key can then restore it by loading the encrypted backup into the device. If the device itself is destroyed, the manufacturer may be able to supply another one with the same internal information, thus allowing recovery of the key.

View All Answers

**Question - 3:**

How Are Certifying Authorities Susceptible to Attack?

**Ans:**

One can think of many attacks aimed at certifying authorities, all of which can be defended against.
For instance, an attacker may attempt to discover the private key of a certifying authority by reverse engineering the device in which it is stored. For this reason, a certifying authority must take extreme precautions to prevent illegitimate access to its private key;
The certifying authority's key pair might be the target of an extensive cryptanalytic attack. For this reason, CAs should use long keys, and should also change keys regularly. Top-level certifying authorities need especially long keys, as it may not be practical for them to change keys frequently because the public key may be written into software used by a large number of verifiers.

View All Answers

**Question - 4:**

How Do Certifying Authorities Store their Private Keys?

**Ans:**

It is extremely important that the private keys of certifying authorities are stored securely because compromise would enable undetectable forgeries. One way to achieve the desired security is to store the key in a tamper-resistant device. The device should preferably destroy its contents if ever opened, and be shielded against attacks using electromagnetic radiation. Not even employees of the certifying authority should have access to the private key itself, but only the ability to use the private key in the process of issuing certificates.

View All Answers

**Question - 5:**

Who Issues Certificates and How?

**Ans:**

Certificates are issued by a certifying authority (CA), which can be any trusted central administration willing to vouch for the identities of those to whom it issues certificates and their association with a given key. A company may issue certificates to its employees, a university to its students, a town to its citizens. In order to prevent forged certificates, the CA's public key must be trustworthy: a CA must either publicize its public key or provide a certificate from a higher-level CA attesting to the validity of its public key. The latter solution gives rise to hierarchies of CAs. See Figure 14 for an example.

View All Answers

### Question - 6:

How are Certificates Used?

### Ans:

Certificates are typically used to generate confidence in the legitimacy of a public key. Someone verifying a signature can also verify the signer's certificate, to ensure that no forgery or false representation has occurred. These steps can be performed with greater or lesser rigor depending on the context.

The most secure use of authentication involves enclosing one or more certificates with every signed message. The receiver of the message would verify the certificate using the certifying authority's public key and, now confident of the public key of the sender, verify the message's signature. There may be two or more certificates enclosed with the message, forming a hierarchical chain, wherein one certificate testifies to the authenticity of the previous certificate. At the end of a certificate hierarchy is a top-level certifying authority, which is trusted without a certificate from any other certifying authority. The public key of the top-level certifying authority must be independently known, for example, by being widely published.

**View All Answers**

### Question - 7:

What are Certificates?

### Ans:

Certificates are digital documents attesting to the binding of a public key to an individual or other entity. They allow verification of the claim that a given public key does in fact belong to a given individual. Certificates help prevent someone from using a phony key to impersonate someone else.

**View All Answers**

### Question - 8:

What are the Best Factoring Methods in Use Today?

### Ans:

Factoring is a very active field of research among mathematicians and computer scientists; the best factoring algorithms are mentioned below with some references and their big-O asymptotic efficiency. O notation measures how fast an algorithm is; it gives an upper bound on the number of operations (to order of magnitude) in terms of n, the number to be factored, and p, a prime factor of n.

Factoring algorithms come in two flavors, special purpose and general purpose; the efficiency of the former depends on the unknown factors, whereas the efficiency of the latter depends on the number to be factored. Special-purpose algorithms are best for factoring numbers with small factors, but the numbers used for the modulus in the RSA system do not have any small factors. Therefore, general-purpose factoring algorithms are the more important ones in the context of cryptographic systems and their security.

**View All Answers**

### Question - 9:

Has Factoring Been Getting Easier?

### Ans:

Factoring has become easier over the last 15 years for two reasons: computer hardware has become more powerful, and better factoring algorithms have been developed.

Hardware improvement will continue inexorably, but it is important to realize that hardware improvements make RSA more secure, not less. This is because a hardware improvement that allows an attacker to factor a number two digits longer than before will at the same time allow a legitimate RSA user to use a key dozens of digits longer than before; a user can choose a new key a dozen digits longer than the old one without any performance slowdown, yet a factoring attack will become much more difficult. Therefore, although the hardware improvement does help the attacker, it helps the legitimate user much more. This general rule may fail in the sense that factoring may take place using fast machines of the future, attacking RSA keys of the past; in this scenario, only the attacker gets the advantage of the hardware improvement. This consideration argues for using a larger key size today than one might otherwise consider warranted. It also argues for replacing one's RSA key with a longer key every few years, in order to take advantage of the extra security offered by hardware improvements. This point holds for other public-key systems as well.

**View All Answers**

### Question - 10:

What is the Significance of Factoring in Cryptography?

### Ans:

Factoring is the underlying, presumably hard problem upon which several public-key cryptosystems are based, including RSA. Factoring an RSA modulus would allow an attacker to figure out the private key; thus, anyone who can factor the modulus can decrypt messages and forge signatures. The security of RSA depends on the factoring problem being difficult and the presence of no other types of attack. Unfortunately, it has not been proven that factoring must be difficult, and there remains a possibility that a quick and easy factoring method might be discovered , although factoring researchers consider this possibility remote.

**View All Answers**

### Question - 11:

What is the Factoring Problem?

### Ans:

Factoring is the act of splitting an integer into a set of smaller integers (factors) which, when multiplied together, form the original integer. For example, the factors of 15 are 3 and 5; the factoring problem is to find 3 and 5 when given 15. Prime factorization requires splitting an integer into factors that are prime numbers; every integer has a unique prime factorization. Multiplying two prime integers together is easy, but as far as we know, factoring the product is much more difficult.

**View All Answers**

### Question - 12:

What is an Undeniable Signature Scheme?

### Ans:

Undeniable signature scheme, devised by Chaum and van Antwerpen [CV90][CV92], are non-self-authenticating signature schemes, where signatures can only be verified with the signer's consent. However, if a signature is only verifiable with the aid of a signer, a dishonest signer may refuse to authenticate a genuine document. Undeniable signatures solve this problem by adding a new component called the disavowal protocol in addition to the normal components of signature and verification.

View All Answers

**Question - 13:**

What is a one-time signature scheme?

**Ans:**

A one-time signature scheme allows the signature of only a single message using a given piece of private (and public) information. One advantage of such a scheme is that it is generally quite fast. However, the scheme tends to be unwieldy when used to authenticate multiple messages because additional data needs to be generated to both sign and verify each new message. By contrast, with conventional signature schemes like RSA

View All Answers

**Question - 14:**

What are Certificate Revocation Lists (CRLs)?

**Ans:**

list of certificates who have been reovoked access.
It is use in X.500

View All Answers

**Question - 15:**

Explain (1/10)18 - (1/10)20 = ?

**Ans:**

(1/10)^18 - (1/10)^20
= 1/(10^18) - 1/(10^20)
= (10^2 - 1)/(10^20)
= 99/(10^20)

View All Answers

**Question - 16:**

What is a digital signature?

**Ans:**

A digital signature consists of text that is encrypted using the private key of a public key[md]private key pair. The public key is used to decrypt the signature to verify its authenticity.

View All Answers

**Question - 17:**

Suppose Pipe A can fill in 20 minutes and Pipe B in 30 mins and Pipe C can empty the same in 40 mins. If all of them work together, find the time taken to fill the tank?

**Ans:**

a fill - 1/20 per minute
b fill - 1/30 per minute
c can empty - 1/40 per minute
Suppose this take x minute

```
1 x +1x - 1x
---  --  ----  =1
20   30   40
```

Solve this x=17(approximately)

View All Answers

# Cryptography Most Popular & Related Interview Guides

1 : Cryptography General Interview Questions and Answers.

**2 :** Typesetter Interview Questions and Answers.

**3 :** Ciphers Interview Questions and Answers.

**4 :** Cryptography Teacher Interview Questions and Answers.

**5 :** Typewriter Interview Questions and Answers.

**6 :** Cryptography Interview Questions and Answers.

**7 :** Encryption Decryption 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**