Question 1: Explain the role of Certificate Authority in transmitting digital information through the mechanism of cryptography.

Ans: A Certificate Authority (CA) (or Certification Authority) is an entity that issues digital certificates.

The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified.

In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate.

In the context of a website, when we use the term digital certificate we often refer to SSL certificates. The CA is the authority responsible for issuing SSL certificates publicly trusted by web browsers.

Anyone can issue SSL certificates, but those certificates would not be trusted automatically by web browsers. Certificates such as these are called self-signed. The CA has the responsibility to validate the entity behind an SSL certificate request and, upon successful validation, the ability to issue publicly trusted SSL certificates that will be accepted by web browsers. Essentially, the browser vendors rely on CAs to validate the entity behind a web site.

A CA is responsible for issuing certificates. CA issues the digital certificate based on the recommendation of RA. This digital certificate is signed by the CA using its own private key. The CA issues the certificate which contains the public key of the party who owns the certificate. Certificates have to be purchased from the CA. CA can issue a certificate only after it confirms all the credentials to prove your identity. Once identity is proved, it stamps the certificate to prevent modifications of the details contained in the certificate. CA is analogous to a passport agency. An individual or organization may have any number of certificates issued by different CAs. Different web applications may insist to use a particular certificate. For example, a particular bank may insist to use a certificate issued by that bank for a secured transaction, whereas some other web site may accept any certificate issued by any CA.

Registration Authority (RA) is a third-party verification agency for a Certificate Authority (CA), to perform the verification of the organization or individuals who have applied for the certificate. Final component of the PKI is the Certificate Management System (CMS) through which certificates are published, renewed, or revoked. Examples of Certificate Authority (CA) include Verisign, Thawte, SSL.com, RapidSSL, Network Solutions, GlobalSign, Digicert, Enutrust.net, PinkRoccade, and PKI.CAcert.

Digital Certificate provides an electronic identity to conduct secure transactions by providing your identity (authentication). It is similar to a passport or driver’s license. With a digital certificate, an organization or an individual can provide authentication for all the transactions with friends, business partners, and other online services. Digital certificate assures identity among all the parties involved in the transactions. The most widely used format of a digital certificate is as defined by the CCITT X.509 standards. Digital certificate uses public key cryptography to verify the integrity of the certificate itself.

Question 2: How do search engines work?

Ans: All search engines work using a 3 phase approach to managing, ranking and returning search results. But a lot of people have no idea what is happening behind that search box when they type in their search queries.