**Difference between cloud and data center:**

The main difference between the public cloud and a data center is where the data is stored. In a data center, data is most often stored on the premises of your organization. Some data centers may be in locations not owned by your organization—in this case, **your data center is colocated, but not in the cloud**

**Difference between file-based encryption and full-disk encryption:**

Unlike full-disk encryption, each file in a disk/drive can be encrypted with a different key.

Files that are encrypted using FBE require the key to be decrypted even if the device is unlocked. Encrypted files sent to other devices will stay encrypted till the encryption password/key is entered. So, this keeps data in motion as well as in rest secured.

one of the major drawbacks of FDE is that once the device is unlocked, pretty much all the data in it is accessible. Assume a simple scenario where you leave your unlocked devices somewhere, then anyone can access the data stored in them.

**Which is the best encryption algorithm in cloud cryptographic:**

The best?

According to which parameter? safety? velocity?

You Has received some recommendations such as DES, AES, ECC, Low Weight Ciphers.

I commented that DES is not safe, it can be violated by brute force.

AES, It is also block, but safer, although vulnerable to power attacks.

ECC employs keys shorter that RSA, But it's slower than AES.

Low weight ciphers are designed for environments with memory or area restrictions, there are several options

What are the most suitable algorithms?

It depends on the parameter you want to prioritize and the application scenario.

For short message encryption (like the keys of other algorithms) and for public key scenario, I suggest ECC

For symmetric key scenario I suggest AES. If you want to increase your resistance against power attacks, balancing the with resistance to other staques (such as linear and differential) you could change your-box for another as proposed in:

**An example of asymmetric cryptography :**

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client’s public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

**Difference between Hashing and Encryption :**

|  |  |  |
| --- | --- | --- |
| **Basis** | **Hashing** | **Encryption** |
| **Definition** | It is a process to convert information to a shorter fixed value known as the key that is used to represent the original information. | It is the process to encode data securely such that only the authorized user who knows the key or password is able to retrieve the original data for everyone else it is just garbage. |
| **Purpose** | The purpose of hashing is indexing and retrieving items from the database. The process is very fast. | The purpose of encryption is to transform data to keep it secret from others. |
| **Reverse Process** | The hash code or key can not be reversed to the original information by any means. It can only be mapped and the hash code is checked if the hash code is the same the information is the same otherwise not. The original information can not be retrieved. | The original information can be easily retrieved if we know the encryption key and algorithm used for encryption. |
| **Secure** | It is more secure in comparison to encryption. | It is less secure in comparison to hashing. |
| **Creation of file** | Generally, it tries to generate a new key for each information passed to the hash function but on rare occasions, it might generate the same key popularly known as a collision. | It will always generate a new key for each information. |
| **Example** | MD5, SHA256 | RSA, AES and Blowfish |
| **Length of information** | The hashed information is generally of small and fixed length. It does not grow with the increase in the information length of information. | The encrypted information is not of fixed length. It grows with the increase in length of information. |