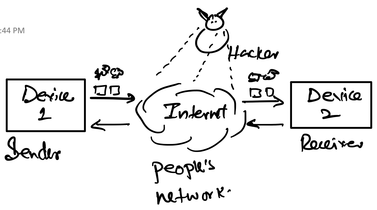
# Encryption

Monday, 19 December 2022 6:44 PM




**Encryption:**

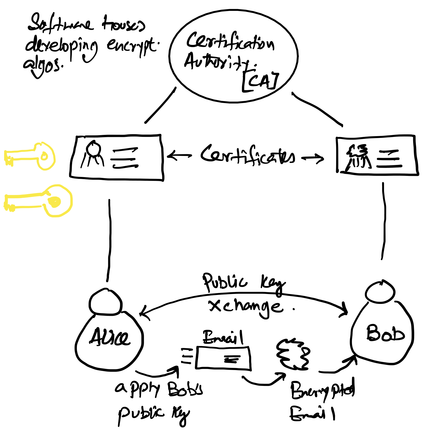
It is a proces to make datas non-understandable for anyone unauthorised for it. Datas needs to be encrypted before it leaves origination and heads to destination using public networks like the Internet.

Encryption uses predefined sophisticated algorithms like MD5 to encrypt datas.

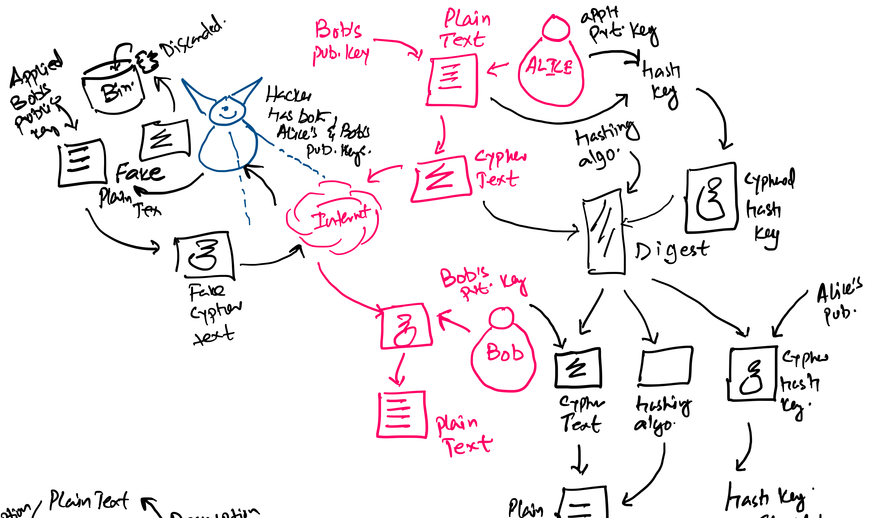
There are many forms of it, but two are more adaptable and used. That is, symmetric and asymmetric.

**ASYMMETRIC:**

Pub. & Pvt. keys can encrypt and decrypt. Both. But one key can't decrypt its own encryption. Only cross-work is acceptable.




Bob will apply this pvt. key to decrypt & read alice's email.




Encryption ( Plain Text → Cypher text ) Decryption

Plain Text → Hash key

Hash key = Should be compared & found to be same. If are not same then sender is Hacker ✗.

- Plain text: Originally produced data, which is not encrypted.
- Cypher text: Encrypted data.
- Encryption: Proces of turning plain text into cypher text.
- Decryption: Proces of turning cypher text into plain text.

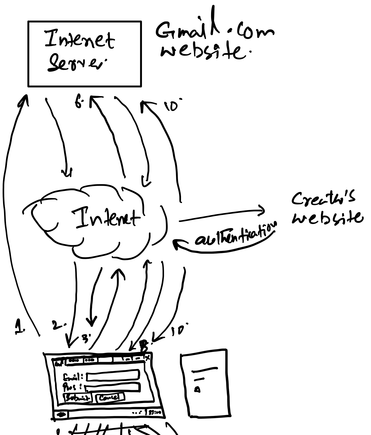
---

Authorisation: It is when you say who you are. Like, username

Authentication: It is when you proof who you are like pws, two factor authentication

---

**SYMMETRIC:**




1. Accessed gmail.com website
2. Website droop its certificate over your comp.
   - Creators datas (CA)
   - Making date
   - Expiry date
   - Owner's ID
   - Sender's Pub. key.
3. Check authenticity
4. Browser generates session key. Session key can encrypt / decrypt. It is alive for one session only. Session is the time we are attached to the website.
5. Your username, pws & sessionkey are all encrypted using gmail.com's public key.
6. Encrypted datas is sent to the server.
7. Server uses its private key to decrypt all 3 datas items. checks username & password to authorise user, and.
8. Send's a welcome message encrypted using User's session key.
9. User's computer will use the session key to decrypt and check the authenticity.
10. Once authorised, the usual communications start and a padlock appears by the website address.