But, Hacker won't stop right there. Erala key a dhan edukka mudila, una fake website ku kondu varen nu solwan.

1) Like original website server sends you a public key to encrypt your symmetric key, Hacker also will develop a fake website, creates a key pair, keep private key with him and sends you public key once you type the website.

2) So, when you type the fake website, you will endup hacked.

How do you identity that balaji can make sure that public key he gets when he types flipkart.com is valid?

Any server that sends the key, it will also send certificates to identity and prove the validness.

Certificate contains - domain name
issued to whom
date of issuing.

How do you verify the certificate? If you generated the certificate and verify it, it is called self-signed certificate

2) But, when famous organizations signed it, it is from trusted CA.

Who verifies the certificate? your browser. All browsers have the ability to verify it. If the fake cert, it will show a warning.

Trusted CA: famous organizations like Digicert, Symmantec, etc.