

HTTPS

HTTPS

- What is this?
 - Default port?
-

Public Key Infrastructure (PKI)

- two separate keys
 - Ingredients to PKI
 - Plaintext
 - Encryption Algorithm
 - Public and private key
 - Each user generates a pair, public key is publicly available
 - Certificate
 - Certificate Authority
-

PKI More

- encrypt message using persons public key, only corresponding private key can decrypt
 - private keys are never distributed
 - can ensure a person is who they say they are
 - when sending messages we can ensure confidentiality
 - [Video](#)
-

Digital Certificates

- downside: some user could send their public key, purporting to be Bob.
 - solution is public key certificate
 - consists of public key, userid, plus signed by trusted 3rd party (CA)
 - A CA:
 - Issues, revokes, distributes digital certs (Digicert, Verisign)
 - Should be trusted
-

More stuff that you didn't want to know

- We have been talking a lot about keys, but the keys are just used for encryption/decryption as part of an algorithm to encrypt/decrypt data. Some of these algorithms are:
 - RSA
 - DSA
 - ECC
 - You can see what algorithm is used by looking at the cert.
-

Our methodology

Essentially we will use something like `letsencrypt` which will generate our public/private keys, send a csr to the CA, get the cert, and install it so that apache is aware of it.

One more note

Our browser likely won't trust certificates signed by `letsencrypt` unless we specifically tell the browser that it should be trusted.