- Public Key

- Private Key

- Signed Secret

Signed Secret.
- Very Crash
- Obvious Reason
- Blue Sandwich
- Time Stamp

- Certificate/Decompress
- Encryption/Decompress

Crytpo Protocols

- 2:30pm
  Reading
If compulsive and resistant (induced) to ask and do so, refer to self-referencing scenario.

- No must
- Read: transfer
- Acknowledge feedback
- Log: debrief
- Proc. Phase

Ab to court (induced)
Self-efficacy - 8 & every step
From the message, another message man's image.

- Identification
- Integrity
- Authenticity
- Privacy

Other properties.
- Access Control
- Availability / Reliability
Cryptographic Protocol

**KERBEROS** - Controls Access to servers by authorized users

- Symmetric encryption only
- (No pub keys)
Alice Authenticator

// $K_{Alice} =$ hash of password, clear passwd stored @ server

Alice Authenticator $\rightarrow$ Alice

$P_{Alice} \rightarrow TGS$

for Alice $\rightarrow$ TGS

$K_{A-TGS} \rightarrow$ session key

$K_{A-TGS} \rightarrow$ TGS

between Alice & TGS

$K_{Alice} =$ shared key
Alice sends to TGS, to get the session key KA-B, gets timestamp and lifetime.

Session key: Alice, Bob

TGS:
{"Alice", "Bob"}K

A-TGS

//validity = requested lifetime

Server:
Alice:
{ T
TGS, Life, KA-B, “Bob”, “Alice” }K

B-TGS

A-TGS

//timestamp
3. Alice establishes session key with Bob and Bob authenticates himself.

Alice

Bob

TS, L, KA-B, \{ Alice \{ K_{B-TGS}, TA \} \} KA-B

Alice sends TGS \{ TA+1 \} KA-B to Bob.

Bob

Bob to Alice

Alice establishes session key with Bob and Bob authenticates himself.