9. TransPort Layer Security- 765 1.2 and 1.3 HTTP is a Stateles protocol, TCP is stateful Here Plant such manged as moran use I Hence we can use UDP with HTTP. as well de organs with the paint the forest HTTPS almost same as MTTP. Millions 13 1 2 17 Used might sammetrick mitgle on a suction of 22 g HTTPS 1275443 o pen (Handshaka) offst too The goal of this handshake is for the Server and the client to agree on a key. mallo The Symmetric en chyption, Welst. Luncus great And a strong and war fre payload control are control Latency. de cryption TYMORE (gratup) wife way contostauramos Lapzop

if you remember Asymmetric encryption. The message 15 sent by encrypting using public key of the server, by decrypted using the private key of the server,

FLS 1.2 Day Samething Similar. Uses a misd symmetrick assymetric encryption ELLObou Client Hello (1strup) E List of Supported TLS versions. List of supported encryption Algos. · Sorver Hello (2nd toup) Client choose TLS version, tump? choose which enoughtuto doose, Times Sends Servers public Key as well, After getting pullic key of Dervey. the Symmetricker (35dtrip) locked inside the public kep of Serry. Cererates the symmetrickey. W (Symmetric) (Pullickey Lock) Server gives (4th tourp) final Ack to start communication

21111

feren.

Server private Key to deoxypt the message

Problem with TES1-2 * S2nd trip and 371d trip} You are sending public key of server [Cert] and the 59 mmetric key across, If someone sniffs it and get control over the private keyof the Server. Boom Boys Grang Charl Is Leaked 2 Insecure. & Refore leggi beginning to chart, y Round trips have to le made in order to Starte actual commis. the Problem of wint I breen to Hence TLS 1-2 is slow. faron the combination. Diffie Hellman Private Tclient (Don't send) Cambine three we get the the connection symmetric key C Don't Sudport for less thankfor (bound o 12 dans and 15

