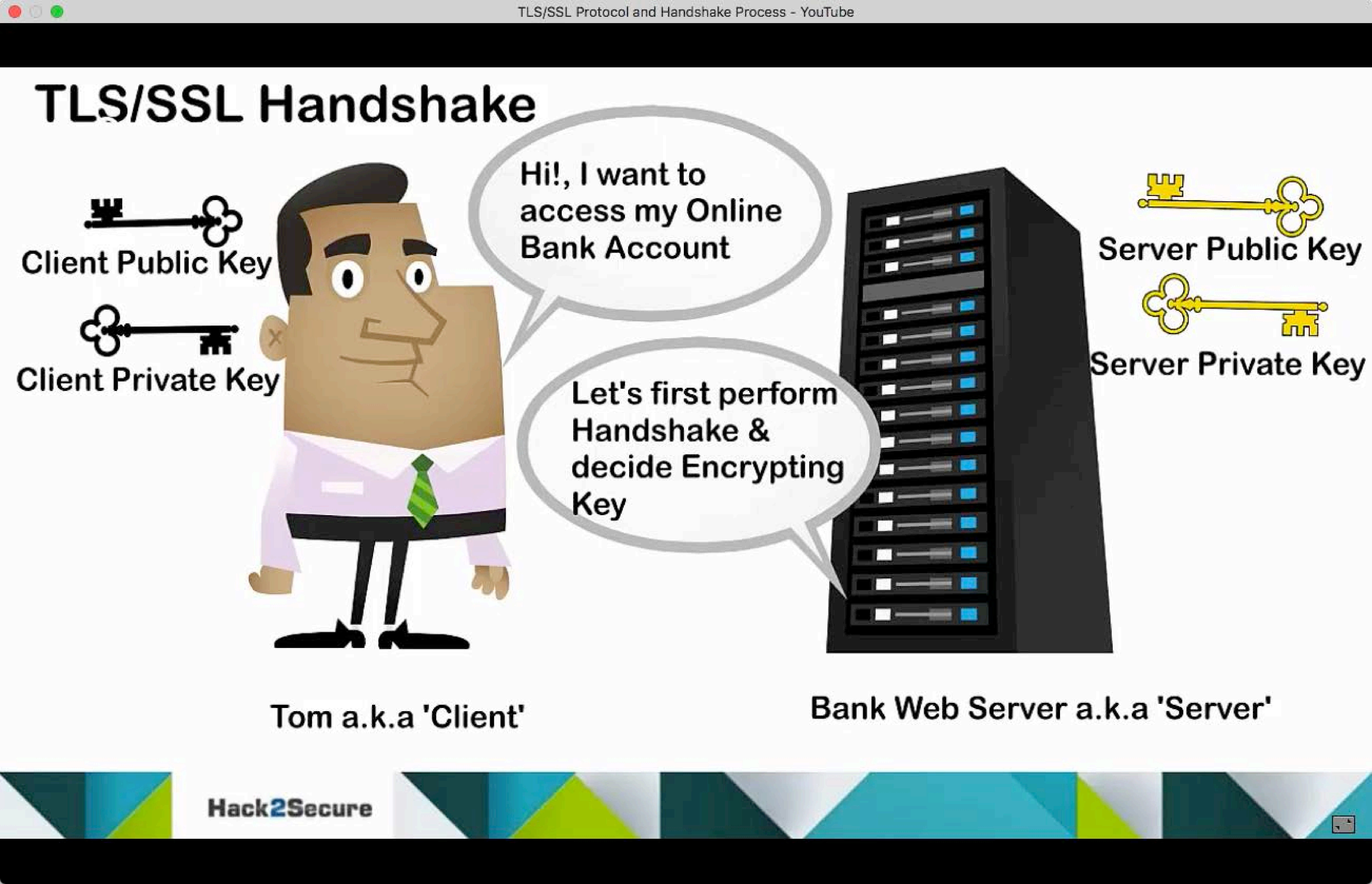


TLS/SSL Protocol and Handshake Process - YouTube

TLS/SSL Handshake

Hi!, I want to access my Online Bank Account

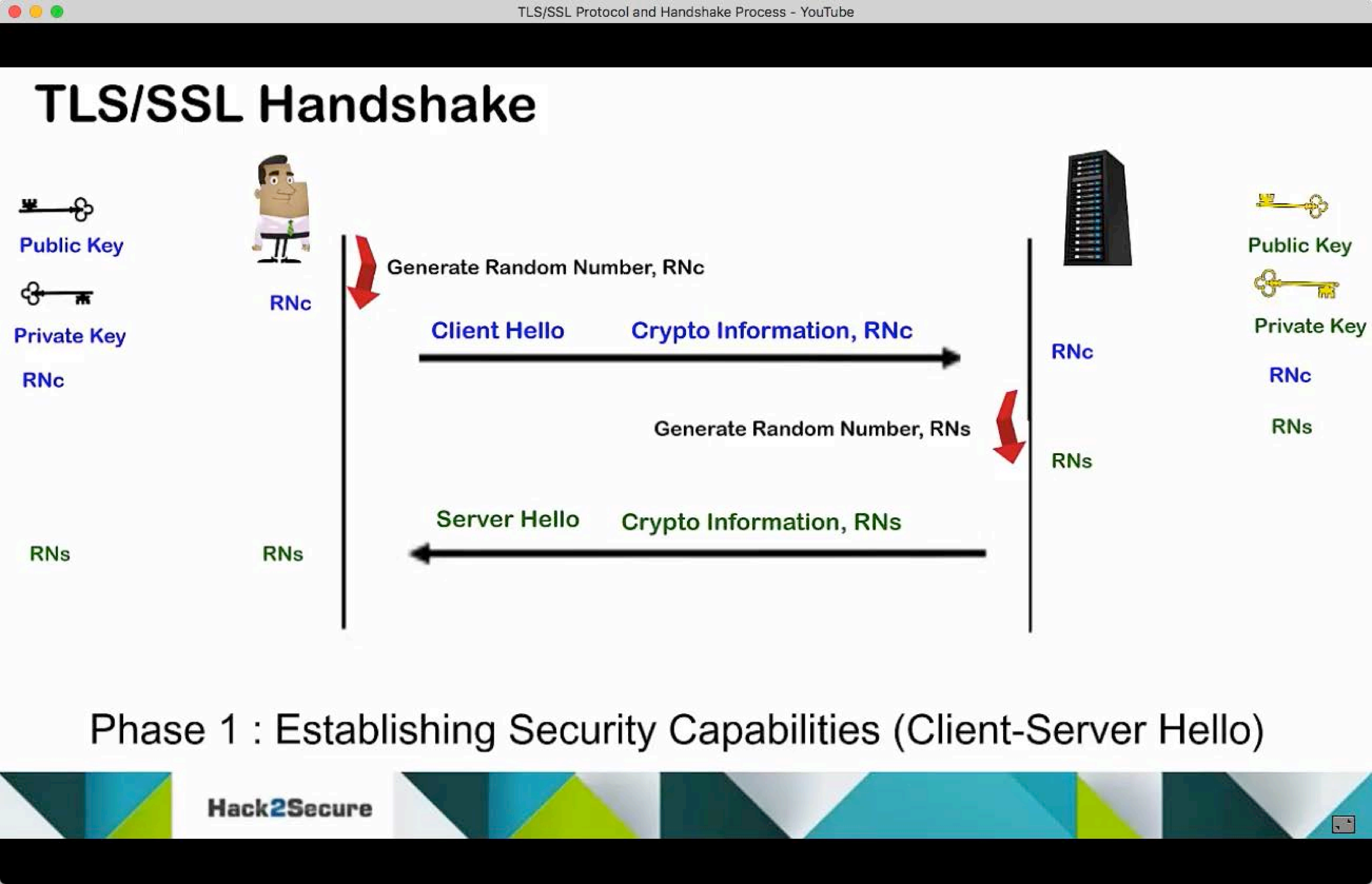
Let's first perform Handshake & decide Encrypting Key

Tom a.k.a 'Client'

Bank Web Server a.k.a 'Server'

Hack2Secure

TLS/SSL Protocol and Handshake Process - YouTube



TLS/SSL Handshake

Public Key

Private Key

RNc

RNs

RNc

RNs

Generate Random Number, RNc

Client Hello Crypto Information, RNc

RNc

Generate Random Number, RNs

RNs

Server Hello Crypto Information, RNs

Public Key

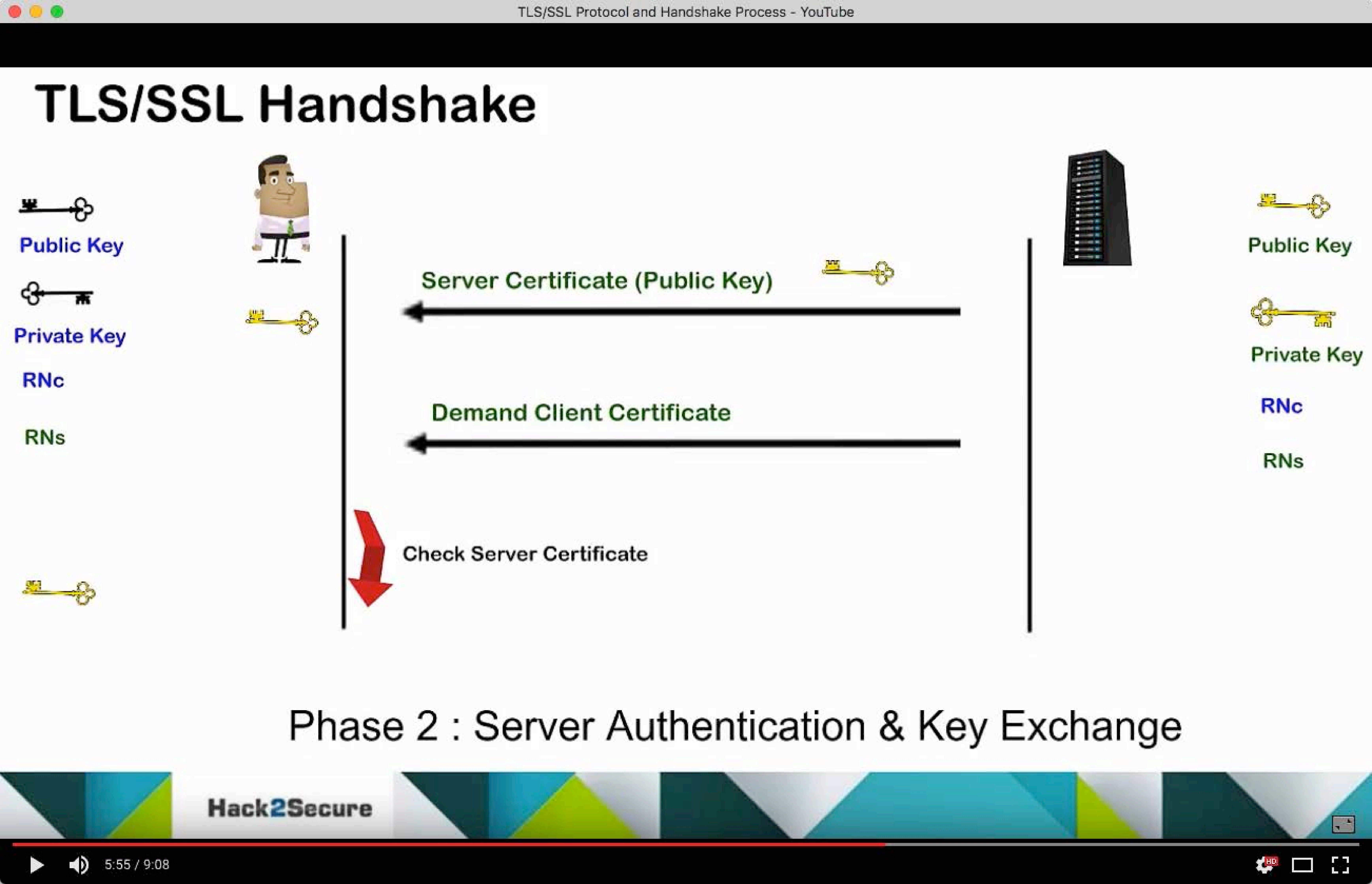
Private Key

RNc

RNs

Phase 1 : Establishing Security Capabilities (Client-Server Hello)

Hack2Secure



TLS/SSL Protocol and Handshake Process - YouTube

TLS/SSL Handshake

Public Key

Private Key

RNc

RNs

Server Certificate (Public Key)

Demand Client Certificate

Check Server Certificate

Public Key

Private Key

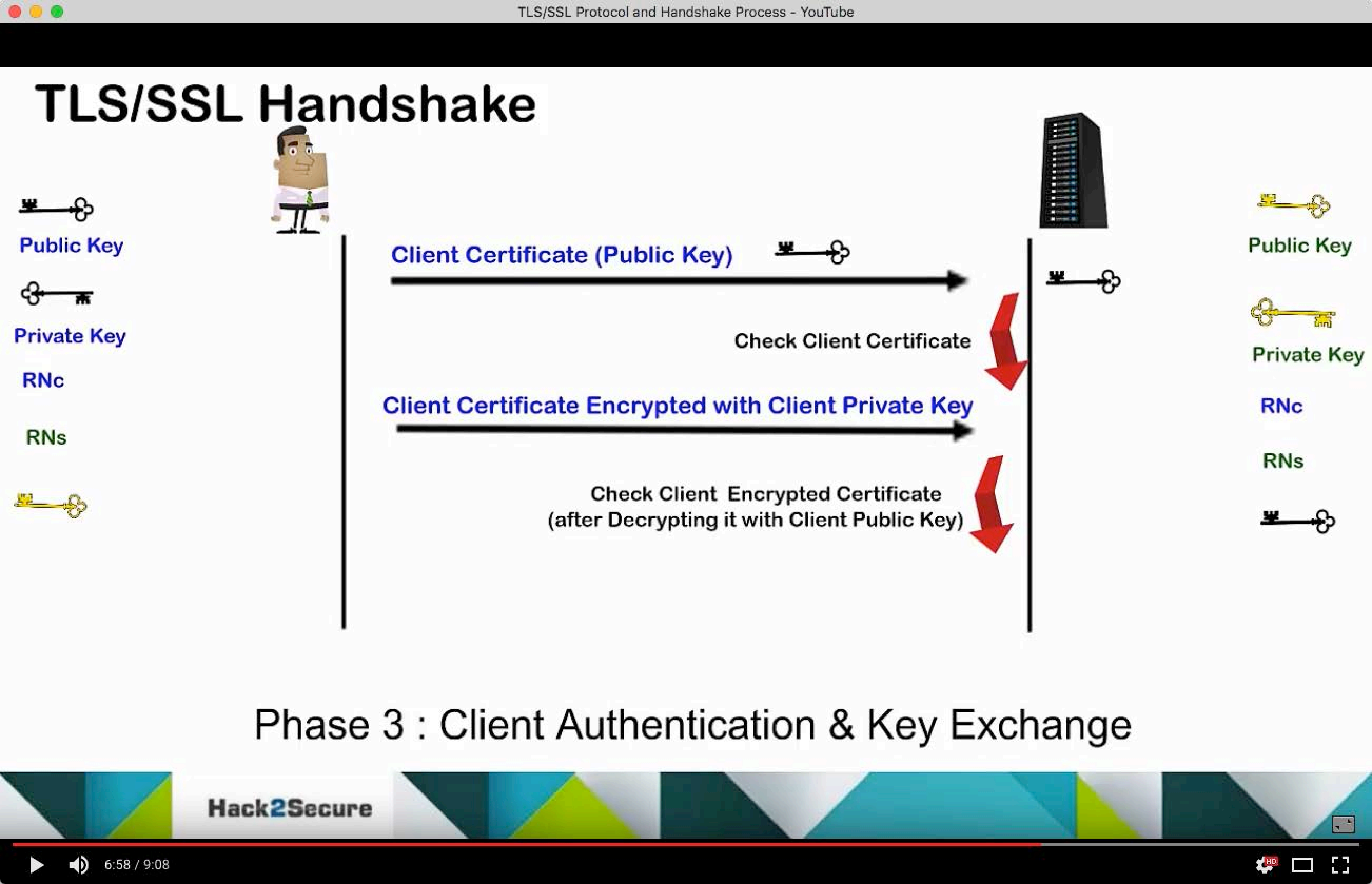
RNc

RNs

Phase 2 : Server Authentication & Key Exchange

Hack2Secure

5:55 / 9:08



TLS/SSL Handshake

Public Key

Private Key

RNc

RNs

Client Certificate (Public Key)

Check Client Certificate

Client Certificate Encrypted with Client Private Key

Check Client Encrypted Certificate
(after Decrypting it with Client Public Key)

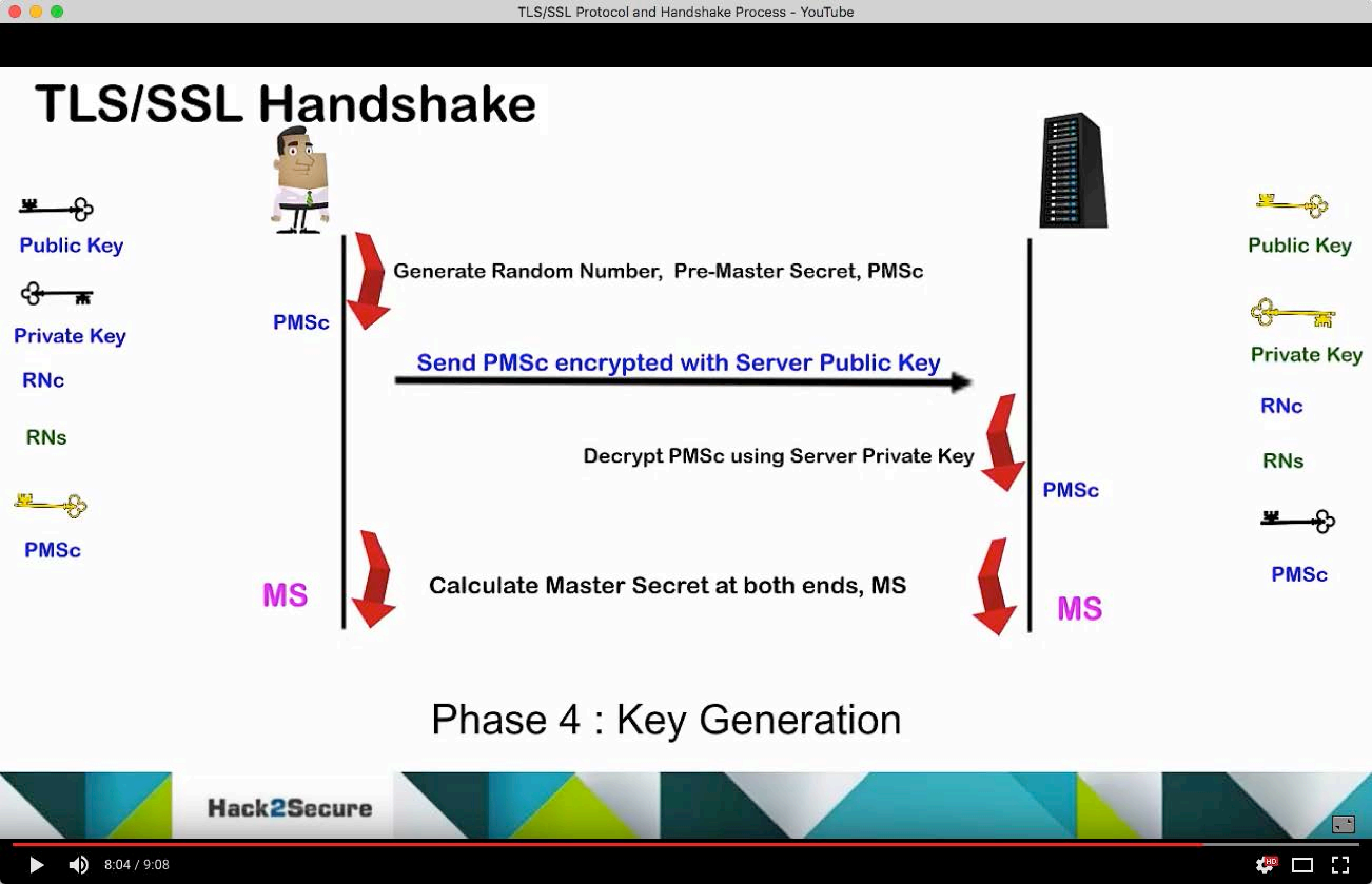
Public Key

Private Key

RNc

RNs

Phase 3 : Client Authentication & Key Exchange



TLS/SSL Protocol and Handshake Process - YouTube

TLS/SSL Handshake

Public Key

Private Key

RNc

RNs

PMSc

PMSc

Generate Random Number, Pre-Master Secret, PMSc

Send PMSc encrypted with Server Public Key

Decrypt PMSc using Server Private Key

PMSc

Calculate Master Secret at both ends, MS

MS

MS

Public Key

Private Key

RNc

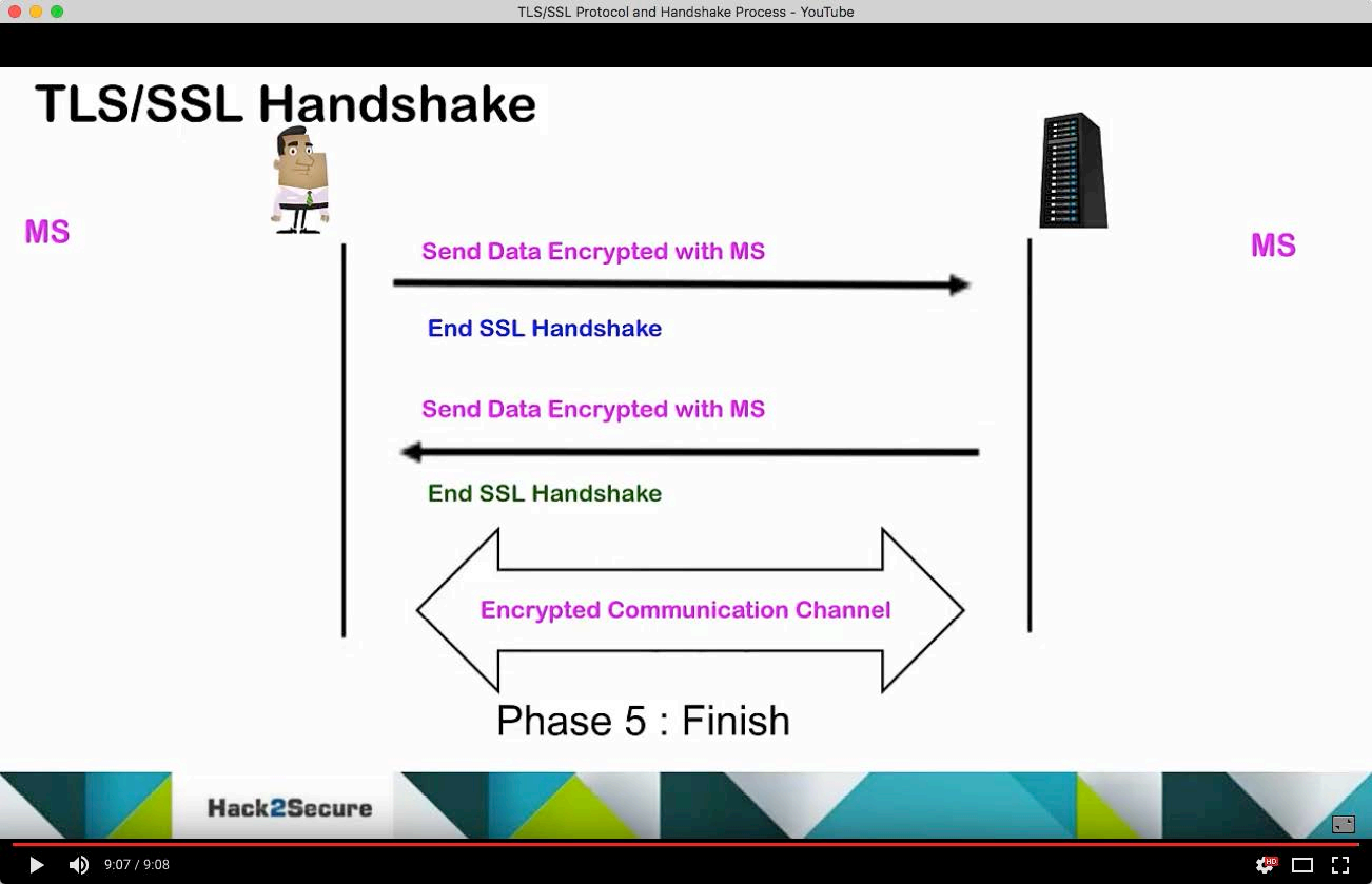
RNs

PMSc

Phase 4 : Key Generation

Hack2Secure

8:04 / 9:08



TLS/SSL Protocol and Handshake Process - YouTube

TLS/SSL Handshake

MS

MS

Send Data Encrypted with MS

End SSL Handshake

Send Data Encrypted with MS

End SSL Handshake

Encrypted Communication Channel

Phase 5 : Finish