No Secret is found by Server

Client -> Hostname, N1, “PHASE2”, HMAC(Hostname, secret) -> Server

\*\*Server Checks HMAC

Client <- “PHASE1” <- Server

Client -> “p,g” -> Server

Client <- “g­­b mod p” <- Server

Client -> “ga mod p” -> Server

Client <- “PHASE2” <- Server

Client <- FSecret(N2+N1, N2) <-Server

\*\*Client checks math

Client -> FSecret(N2+N3, N3) -> Server

\*\*Server checks math

*Phase 3 Starts*

Client -> F­Secret(IV, Session Key)(Log) -> Server

No Secret is found by Client

Client -> Hostname, N1, “PHASE1”, HMAC(Hostname, secret) -> Server

\*\*Server Checks HMAC

Client <- “PHASE1” <- Server

Client -> “p,g” -> Server

Client <- “g­­b mod p” <- Server

Client -> “ga mod p” -> Server

Client <- “PHASE2” <- Server

Client <- FSecret(N2+N1, N2) <-Server

\*\*Client checks math

Client -> FSecret(N2+N3, N3) -> Server

\*\*Server checks math

*Phase 3 Starts*

Client -> F­Secret(IV, Session Key)(Log) -> Server

Secret is found by Server and Client

Client -> Hostname, N1, “PHASE1”, HMAC(Hostname, secret) -> Server

\*\*Server Checks HMAC

Client <- “PHASE2” <- Server

Client -> Hostname, N1 -> Server

Client <- “PHASE2” <- Server

Client <- FSecret(N2+N1, N2) <-Server

\*\*Client checks math

Client -> FSecret(N2+N3, N3) -> Server

\*\*Server checks math

*Phase 3 Starts*

Client -> F­Secret(IV, Session Key)(Log) -> Server

Message Encryption:

PHASE 1: Unencrypted (Diffe-hellman)

PHASE 2: AES 256bit ECB

PHASE 3: AES 256bit CBC

Crypto component composition:

IV: SHA256(N2\*N3)16 # 16bit slice

Session Key: SHA256(N2)16­ + SHA256(N3)16