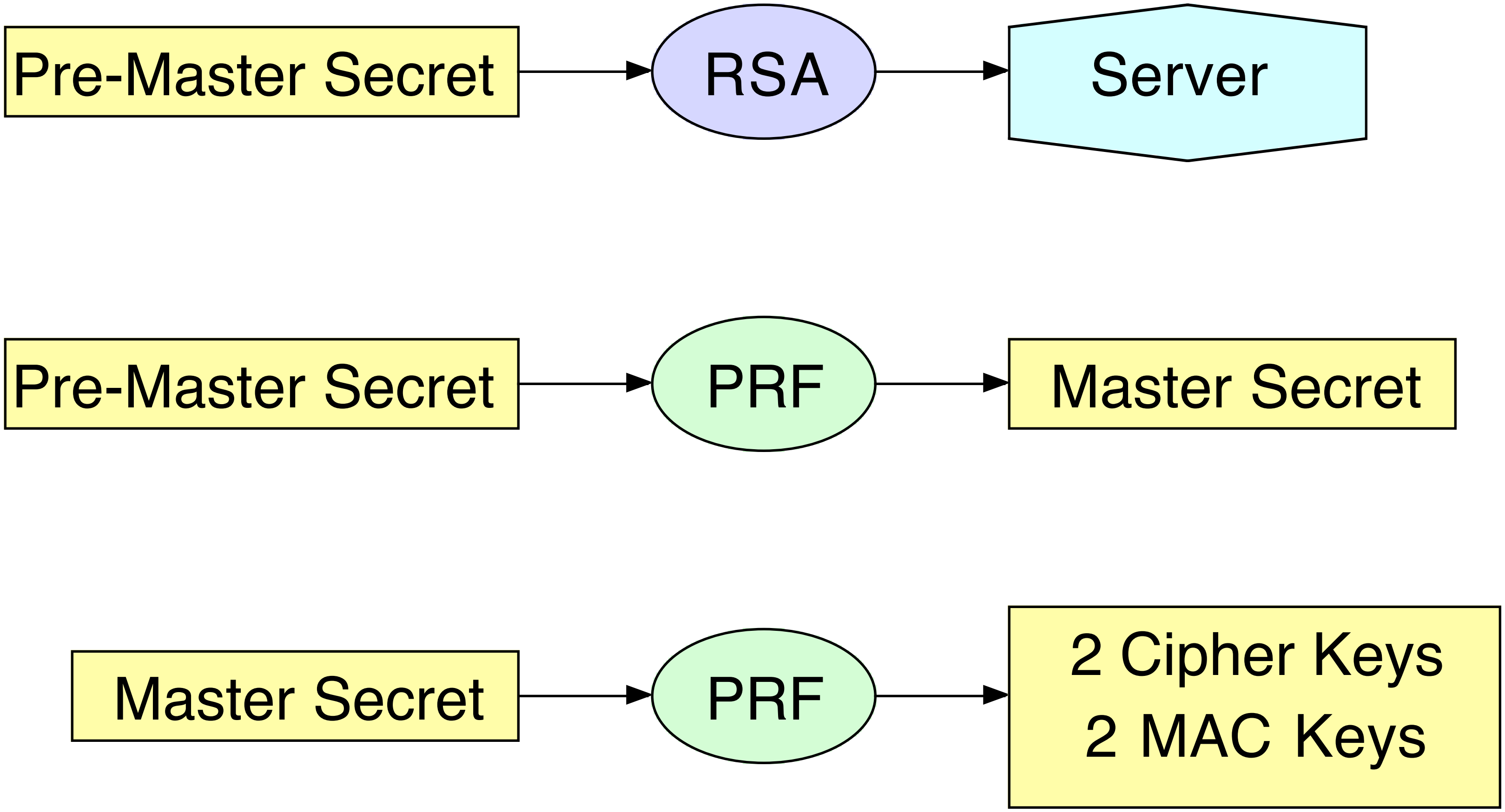
Looking Over Virtual Shoulders
(Shared Generation of SSL Keys)

Hal Finney - PGP Corporation

SSL/TLS Crypto Setup

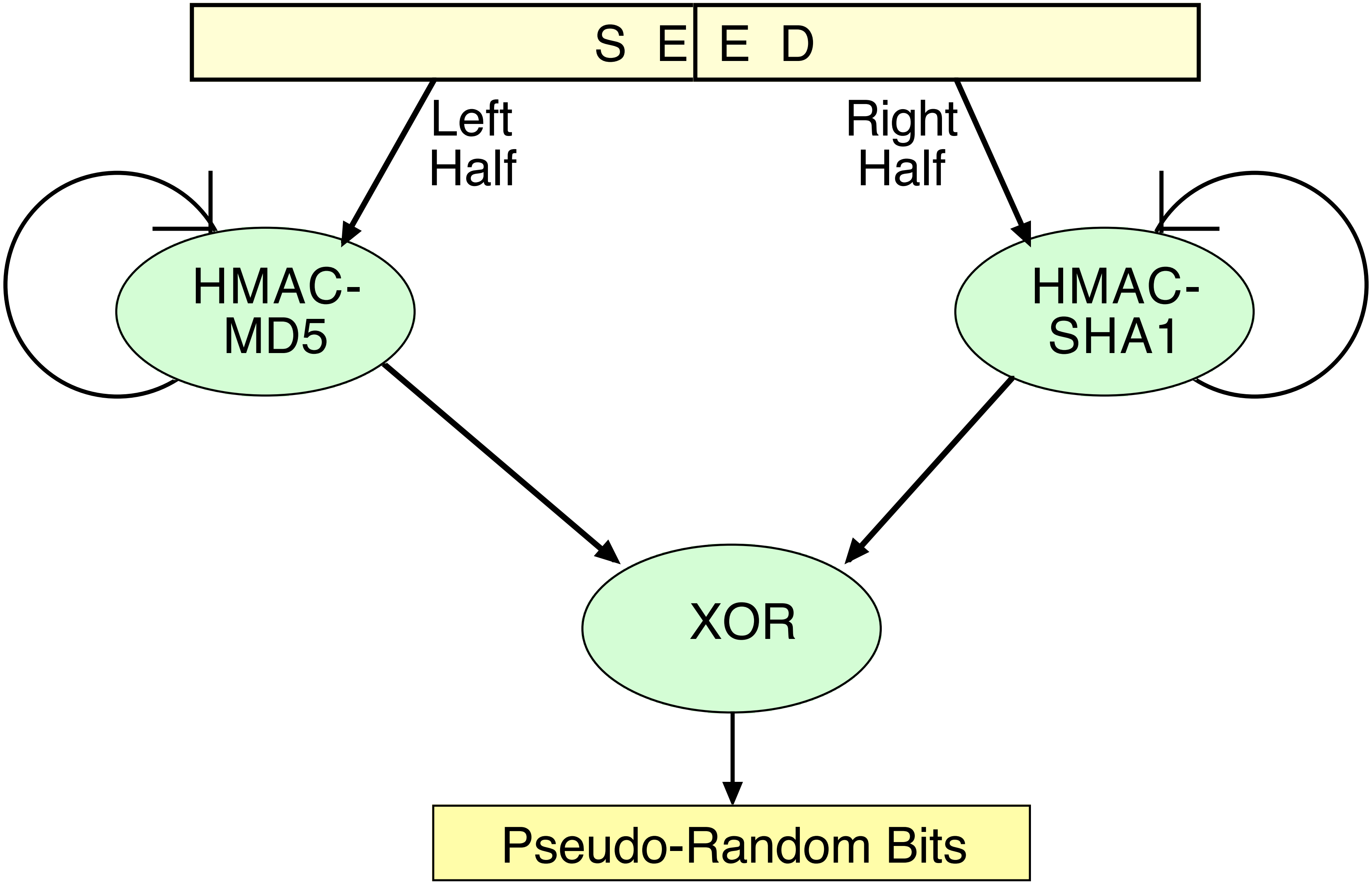


Pre-Master Secret → RSA → Server

Pre-Master Secret → PRF → Master Secret

Master Secret → PRF → 2 Cipher Keys 2 MAC Keys

PRF

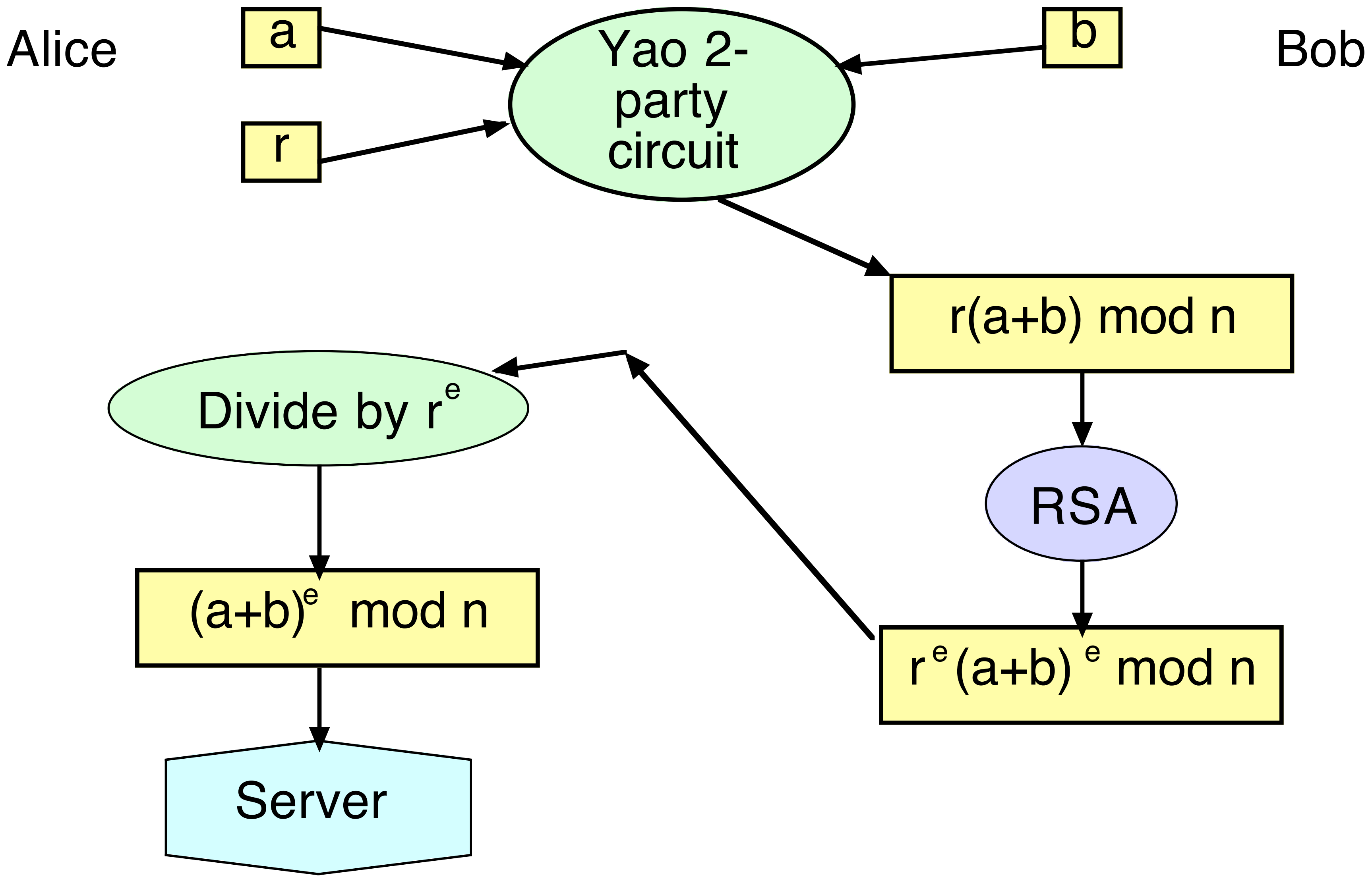

S E E D
Left Half
Right Half
HMAC-MD5
HMAC-SHA1
XOR
Pseudo-Random Bits

Alice and Bob

- Alice chooses left half Pre-Master Secret
- Bob chooses right half PMS
- Mutually RSA-encrypt it
- Alice runs HMAC-MD5 left half of PRF
- Bob runs HMAC-SHA1 right half of PRF
- Combine bits so Alice gets left half Master Secret
- Bob gets right half MS
- Again run PRF left and right halves independently

- Combine bits so Alice gets keys for sending TO server
- Bob gets keys for receiving FROM server
- Alice sends login credentials
- Bob reads server data, is convinced.

RSA Encrypt a+b



Cost and News

- Yao modular multiply implementation tested
- Takes 2 minutes on Mac laptop for 1024 bit modulus
- Takes 300 MB of data exchange
- Can be pre-computed in advance of connection

- Also, TLS 1.2 came out last Friday! RFC 5246
- Replaces left-half/right-half structure
- PRF is just HMAC-SHA256
- Too bad for Alice and Bob!