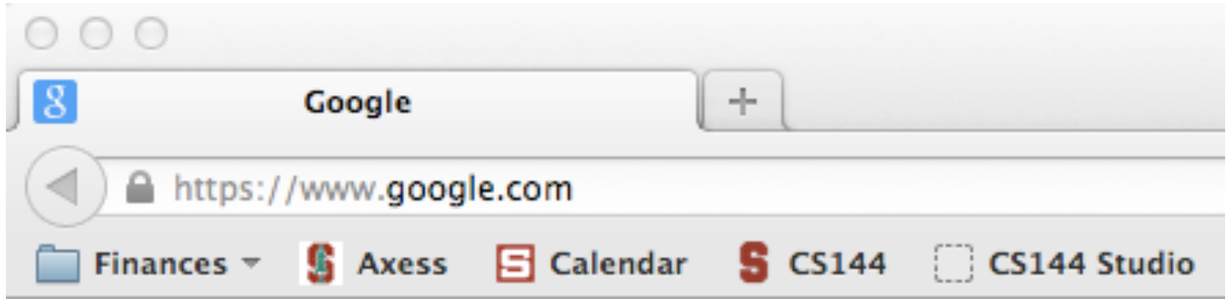
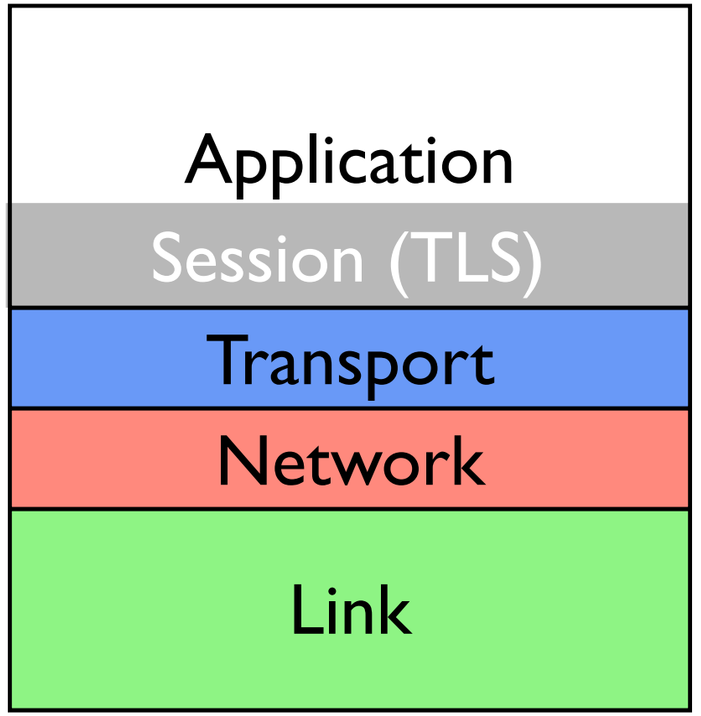
Transport Layer Security (TLS)

RFC5246: you use it every day

Transport Layer Security

- "Transport Layer Security"
- Secure session layer on top of TCP
  - Provides stream abstraction (just like TCP)
  - Add confidentiality, integrity, authenticity
- Most recent version is TLS 1.2, RFC5246
  - Started as Secure Socket Layer (SSL) by Netscape
- Used by HTTPS (lock in browser bar)





What Ciphers to Use

- A TLS session negotiates four ciphers
  - Cipher used for authentication of server and optionally client (RSA, DSS)
  - Cipher used for key exchange (RSA, DHE)
  - Cipher used for symmetric confidentiality (RC4, AES, DES)
  - Cipher used for integrity (HMAC-MD5, HMAC-SHA)
- Negotiated in a 5-step session initiation protocol

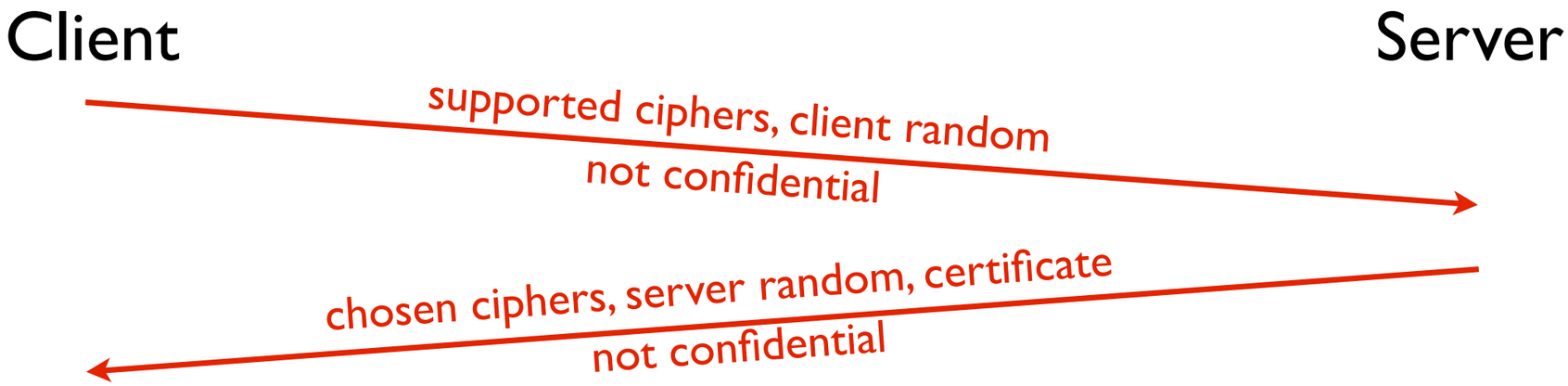
TLS Cipher Negotiation

Client

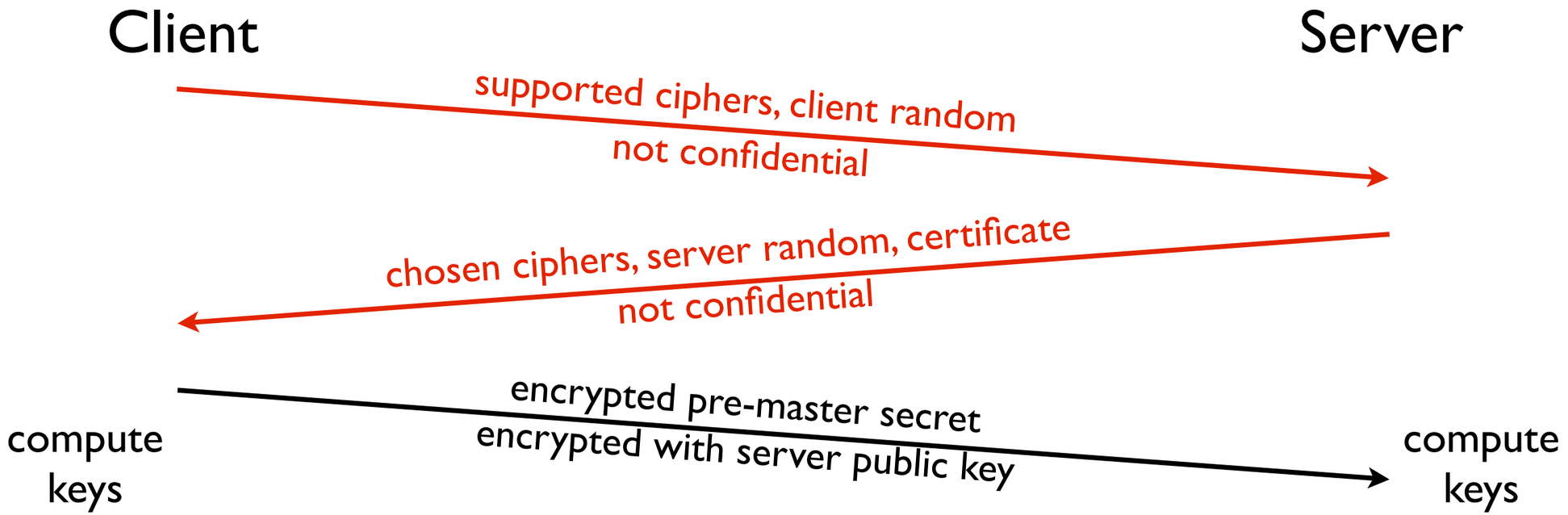
Server

TLS Cipher Negotiation

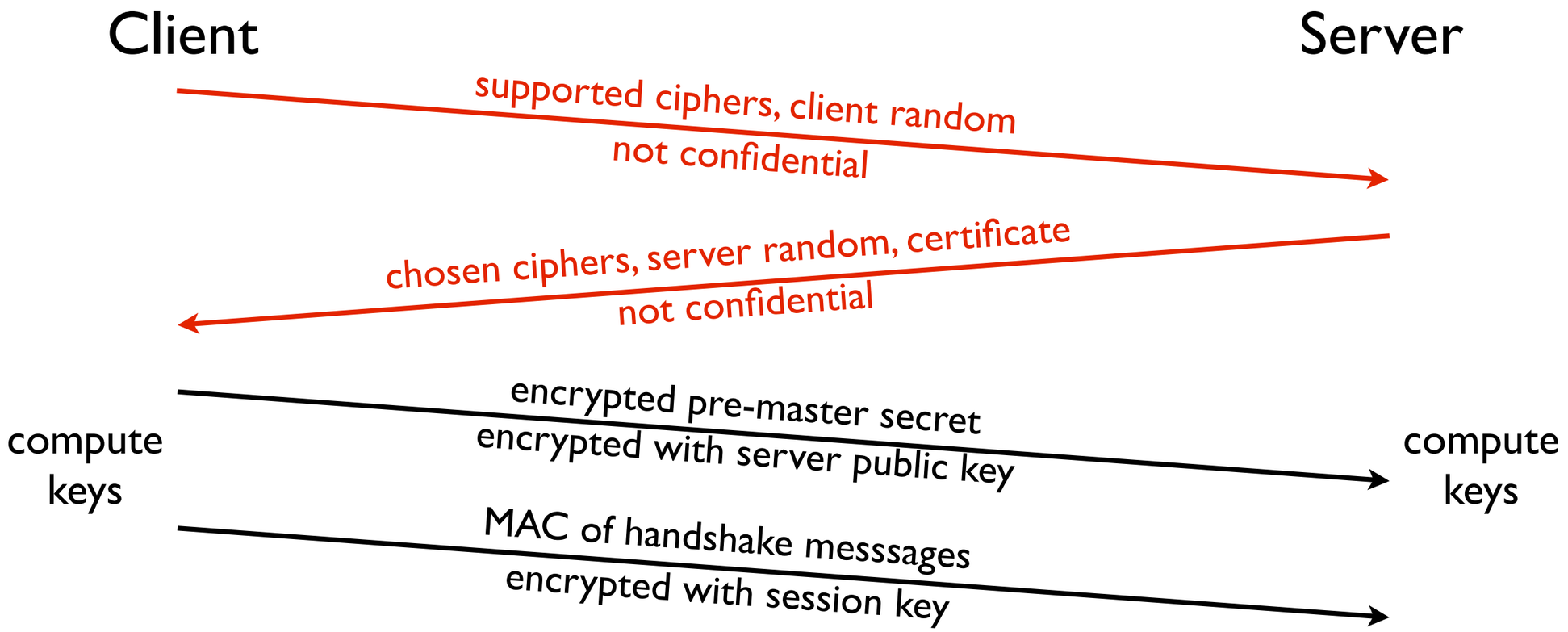
TLS Cipher Negotiation



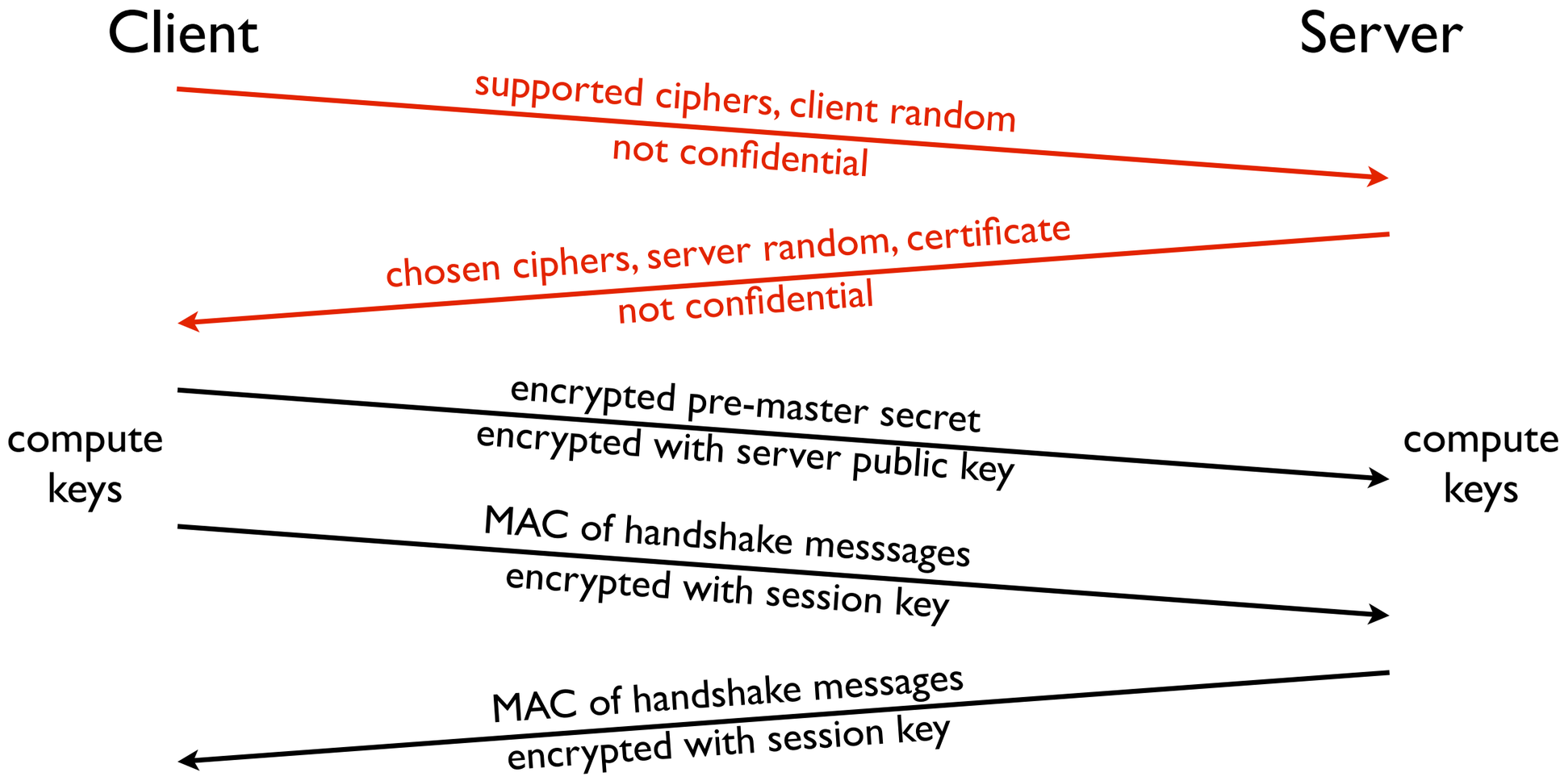
TLS Cipher Negotiation



TLS Cipher Negotiation

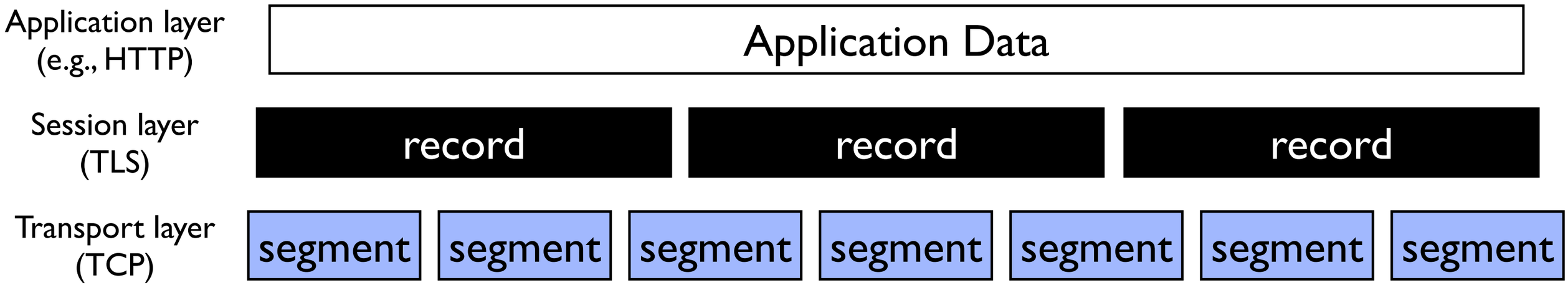


TLS Cipher Negotiation



TLS Message Format

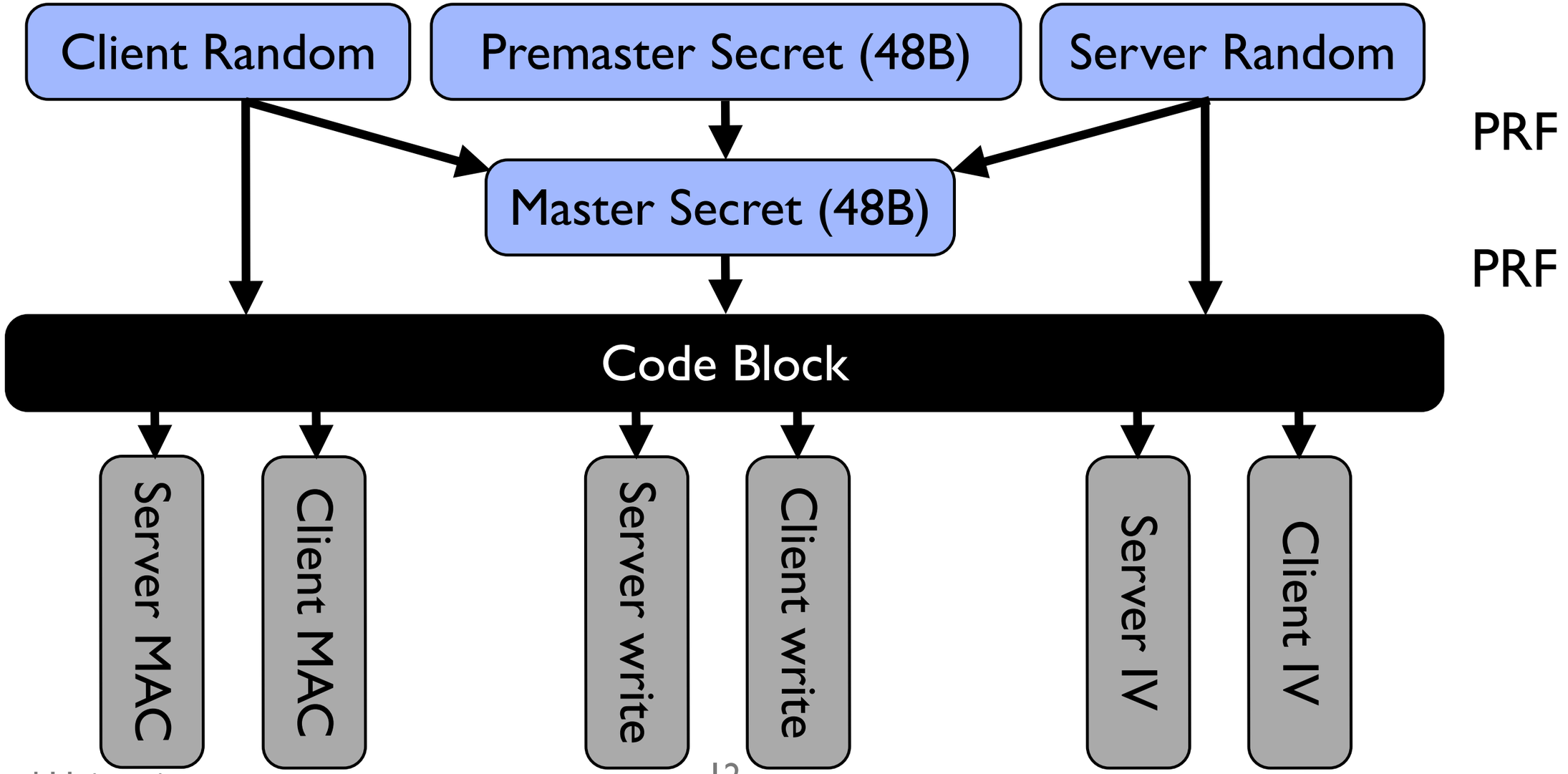
- TLS breaks stream of data from application into records
  - 1-2^{14} bytes in length
  - Records are compressed (default compression algorithm is null)
- Records sent over TCP stream (broken into segments, etc.)



Establishing Session Keys

- Both client and server add randomness
- Client sends "pre-master secret" encrypted with server's public key
- Use randomness and pre-master secret to generate "master secret"
- Use master secret and random numbers to generate session keys
  - Client to server write (encryption)
  - Client to server MAC
  - Server to client write (encryption)
  - Server to client MAC
  - Client initialization vector
  - Server initialization vector
- Support for resuming sessions with same master secret (but new keys)

Session Key Details



Quiz

TLS random values are 32 bytes long (a 4 byte timestamp and 28 bytes of randomness). The premaster secret is 48 bytes long, 2 bytes of protocol version and 46 bytes of randomness. The master secret is 48 bytes long.

Suppose your TLS session uses these to generate 128 bytes of keys. What is the maximum number of tries an adversary might have to make to crack the session keys, assuming an exhaustive attack? Assume that the adversary can correctly recompute the output of a pseudo-random function from its input and it knows what version of TLS is being used.

Write your answer as the base-2 exponent (i.e., if it would take 2^{31} tries, write 31).

Quiz

TLS random values are 32 bytes long (a 4 byte timestamp and 28 bytes of randomness). The premaster secret is 48 bytes long, 2 bytes of protocol version and 46 bytes of randomness. The master secret is 48 bytes long.

Suppose your TLS session uses these to generate 128 bytes of keys. What is the maximum number of tries an adversary might have to make to crack the session keys, assuming an exhaustive attack? Assume that the adversary can correctly recompute the output of a pseudo-random function from its input and it knows what version of TLS is being used.

Write your answer as the base-2 exponent (i.e., if it would take 2^{31} tries, write 31).

The Costs of Layering

- TLS handshake occurs before application data is exchanged
- Virtual hosts are a way so a single web server can respond differently to requests for different host names which map to the same IP address
  - Host: sing.stanford.edu
  - Host: tinyos.stanford.edu
- This can break TLS: how?
  - Server authentication
  - Key exchange
  - Randomness generation
  - Routing handshake messages
  - Premaster secret generation

The Costs of Layering

- TLS handshake occurs before application data is exchanged
- Virtual hosts are a way so a single web server can respond differently to requests for different host names which map to the same IP address
  - Host: sing.stanford.edu
  - Host: tinyos.stanford.edu
- This can break TLS: how?
  - Server authentication
  - Key exchange
  - Randomness generation
  - Routing handshake messages
  - Premaster secret generation

The Costs of Layering

- TLS handshake occurs before application data is exchanged
- Virtual hosts are a way so a single web server can respond differently to requests for different host names which map to the same IP address
  - Host: sing.stanford.edu
  - Host: tinyos.stanford.edu
- This can break TLS: how?
  - Server authentication
  - Key exchange
  - Randomness generation
  - Routing handshake messages
  - Premaster secret generation