```
transcript =
    ClientHelloInner ||
    ServerHello  // but with first last 24 octets of random set to 0

sech_transcript_hash =
    Message-Digest(transcript, algorithm)
```