NTRU CIPHER SUITES FOR TLS
<DRAFT-IETF-TLS-NTRU-00.TXT>

August 8, 2001

Ari Singer
Principal Engineer, NTRU

Purpose of this draft - Why more cipher suites?

- Define the use of NTRU and NSS public-key algorithms in TLS
- Provide computationally efficient key exchange in TLS for wireless and constrained devices
- Provide efficient client authentication in key exchange
- Specify TLS cipher suites that can be used on memory-constrained devices
- Specify TLS cipher suites that are scalable on the server side with a large population of clients

Overview of the Document

- Key exchange algorithms using NTRU certificates signed by NSS or RSA
- Specification of cipher suites using NTRU/NSS with SHA-1 hash algorithm and RC4, 3DES and AES symmetric encryption algorithms
- Support for multiple key strength key exchange – change from current practice
- Published July 3, 2001 – available on IETF web site

TOPICS FOR FUTURE DISCUSSION

- Draft including NTRU and NSS certificate formats and encoding being presented to PKIX WG (draft-ietf-pkix-pkalgs-supp-00.txt)
- Do we want to add support for multiple hash strengths?
- Since NTRU key generation is so fast, do we want to add cipher suites with perfect forward secrecy?

CONTACT INFORMATION

ARI SINGER
PRINCIPAL ENGINEER, NTRU
ASINGER@NTRU.COM

<DRAFT-IETF-TLS-NTRU-00.TXT>