The End of Crypto

The End of Crypto

That's great

It starts with a Morris worm

The End of Crypto

That's great

It starts with a Morris worm

Zeus and Storm and "I love you"

Schneier, Bruce is not afraid

Break of a Clipper chip

Sasser, Blaster, Mydoom

Gauss serves its own needs

Botnets serve their own needs

SMSZombie Zone

Half a million Chinese phones

Debian RNG

Now we've got your secret keys

Centrifuge in a Flame

Stuxnet, Skynet

Government for hire

and a malware site

It's the end of Crypto as we know it

It's the end of Crypto as we know it

It's the end of Crypto as we know it

And I feel fine.

Dancing hamsters coming in a hurry

with the Nimba breathing down your neck

Antivirus software

baffled, trumped, nothing stopped

Look at that, attacking. Fine then!

Buffer overflow

cross site scripting, common primes

It'll do, save yourself, serve yourself

Gauss serves its own needs

Listen to your bits leak

Dummy with the Slammer

and the Hammer and the Zeus, loose

Conficker, reinstall

Hack attack, service pack

Feeling pretty psyched

It's the end of Crypto as we know it

It's the end of Crypto as we know it

It's the end of Crypto as we know it

And I feel fine.

Eurocrypt and Asiacrypt

Indocrypt and Latincrypt

Crypto, Crappycrypt, CT-RSA

TCC, PKC, S&P, FSE

CHES, CCS, Triple-DES, AES

MD4, MD5, MD6, MDn

RSA, DSA, DLP, ECC

SHA-1,

SHA-1, SHA-2,

SHA-1, SHA-2, SHA-3,

SHA-1, SHA-2, SHA-3, SHAmir

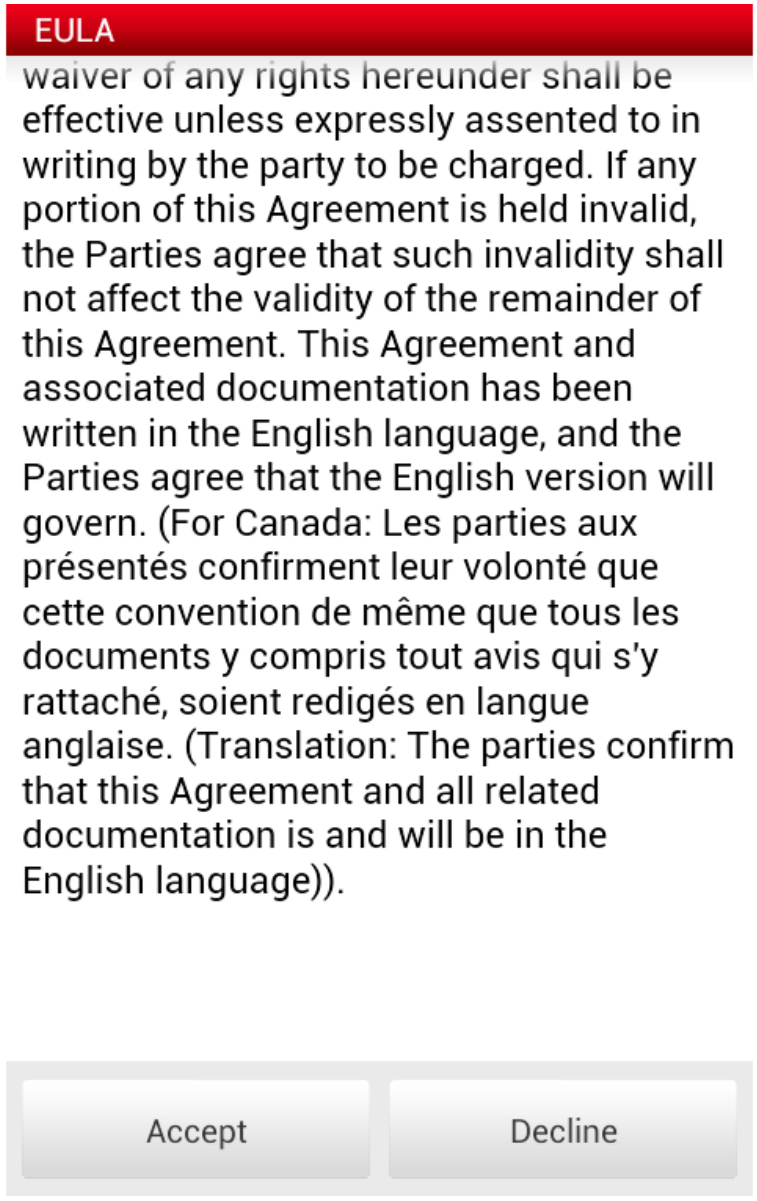
SHA-1, SHA-2, SHA-3, SHAmir

SSH, PKI, X.509

Offer me solutions

offer me alternatives

and I decline.



It's the end of Crypto as we know it

It's the end of Crypto as we know it

It's the end of the net as we know it

And I feel fine.

LinkedIn password leak

Has Sony yet been hacked this week?

RockYou, Yahoo, too

Blizzard runs Diablo

Kindle nooked, 1984—yanked

TCP, PGP, Darpanet, Internet

CIA, NSA, MI6, FBI, BSI, CCR

It's the end of Crypto as we know it

It's the end of Crypto as we know it

It's the end of certificates

as we know them

It's the end of Crypto as we know it

It's the end of certificates

as we know them

It's the end of the end-to-end

as we know it

And I feel fine.

It's the end of Crypto as we know it

It's the end of Crypto as we know it

It's the end of the world as we know it

And I feel fine

It's the IACR as we know it

It's the IACR as we know it

It's the IACR as we know it

And I feel fine