Adam Mulligan

Enigma

Prime Numbers & Cryptosystems

What does that actually

mean?

Key Agreement	Symmetric Ciphers	Authentication	Hashing
RSA	AES	Digital Certificates	SHA family
Diffie-Hellman	Twofish	RSA Signing	Skein

RSA D-H + AES Twofish + Certs Signing + SHA Skein =

?

Wait.

I think that exists.

Where do we stand?

- 6/8 algorithms finished:
    - RSA, DH
    - AES
    - RSA Signing
    - SHA/Skein

- Protocol designed
- Client/server architecture working
- Rough GUI designs complete

Where next?

- Complete remaining algorithms (1-2 weeks from now)
- Finalise protocol and client/server (1-2 weeks from now)
- Finish GUI (By January)
- Integrate all components together (By January)

In the New Year:

- Write report
- Research and implement flaws and attacks