Diffie-Hellman Key Exchange

- A group G and a generator g
- g^A and g^B appear on the wire
- g^{AB} is the shared secret
- Group operation must be easy to compute
- Group representation obscures A and B

D-H with Modular Exponentiation Group

- Group is integers modulo p
- Operation is multiplication
- Elements are bit strings length $log_2(p)$
- E.g. 32 words of 32 bits each
- Optimizations: Karatsuba multiplication Montgomery reduction

Classical D-H Key Exchange

sizes as in recent Photuris drafts

Method: Modular Exponentiation

Params: Mod size M (512 to 1024 bits)

Exp size E (128 to 256 bits)

Compute Time: $M^{1.6}E$

Estimated Best Time: (175MHz 64-bit arch)

10 msec M=512 bits E=128 bits

37 msec M=1024 bits E=160 bits

Keying Material Produced: M bits

Key Strength: theory and measurement yield:

min($\frac{E}{2}$, $2.5\sqrt[3]{M}\,log(M)^{2/3}$ *-15)* bits

Classical D-H Strength

Exp Size	Mod size	Strength
128 bits	512 bits	min(64,53) = 53 bits
160 bits	1024 bits	min(80, 77) = 77 bits

Classical D-H Continued

Attacks:

Pollard-Rho (with Van Oorschot-Wiener)
$3 * 10^{-10} * 2^{E/2}$ mips years

Number Field Sieving (factoring)
$1.5 * 10^{-15} * e^{1.93 log(p)^{1/3} loglog(p)^{2/3}}$
. mips years
based on factoring 119 digit number in 250 MY

Elliptic Curve Groups in Nutshell

$$y^2 = x^3 + ax + b$$

determines a group of points under "addition"

Line PQ intersects curve determining a third point

Reflection of point around x-axis is $P + Q$

Defines commutative group

Point coordinates interpreted over any field

E.g. GF[2^{155}]

Elliptic Curve Key Exchange

(Sizes chosen to match strength of modular exp group in previous slides)

Method: Multiple of elliptic curve point

Params: Field size F, 155 to 256 bits Exponent size E, from 128 to 356 bits

Compute Time: $F^{1.6}E$

Estimated Best Time: (175MHz 64-bit arch)

10 msec F=155 bits E=128 bits
24 msec F=220 bits E=160 bits
(using polynomial representation)

Keying Material Produced: 2F bits

Key Strength: $\frac{E}{2}$ bits

Elliptic Curve D-H Continued

Attacks:

Pollard-Rho (with Van Oorschot-Wiener)
$2 * 10^{-10} * 2^{E/2}$ mips years

Number Field Sieve inapplicable
no notion of "close" points

Perfect forward secrecy Diffie-Hellman exchanges need be only as strong as the required strength of the derived key.

Consider minimal *theoretic* strengths of some algorithms:

DES 2^{55} brute-force, 2^{43} ptxt + ctxt pairs (Matsui)

3DES CBC-inner, mediocre (¡¡ 112 bits), (Biham)
CBC-outer, 2^{64} block cipher

MD5 2^{128} against forgery
2^{64} (in space) against collision

Some observations

D-H computations are expensive

No need to compute more bits than needed for target application

Calculate that need carefully for efficient use of computing resources

Elliptic curves offer good security-to-speed ratio