Diffie-Hellman

Whitfield Diffie

Martin Hellman

Alice & Bob

- Agree on 2 numbers **n** and **g where n is large Prime number**
- **g** is primitive relative mod (n)
- These do not have to kept secret

Alice

- Chooses a large random number **x** such that 0<=x<=n-1
- Calculates

$$X = g^x \bmod (n)$$

- Sends **X, g,** and **n** to Bob.

Bob

- Chooses a large random number **y** such that 0<=y<=n-1
- Calculates

$$Y = g^y \bmod (n)$$

- Sends Y to Alice

Alice

- Calculates

$$k = Y^x \bmod (n)$$

Bob

- Calculates

$$k' = X^y \bmod (n)$$

The Key

- k’ = k is the shared key

$$k = Y^x \bmod (n) = (g^y)^x \bmod (n) = g^{yx} \bmod (n)$$

$$k' = X^y \bmod (n) = (g^x)^y \bmod (n) = g^{xy} \bmod (n)$$

- Nobody can calculate k given n, g, X, and Y

The Key

- Only Alice and Bob know **k**
- Used if you only want a symmetric key

The Key

- Alice and Bob agree to use a prime number p=23 and base g=5. Alice chooses a secret integer ***a*=6**, then sends Bob $\mathbf{A = g^a \bmod p}$
- $A = 5^{\mathbf{6}} \bmod 23$
- A = **15,625** mod 23
- A = 8
- Bob chooses a secret integer ***b*=15**, then sends Alice $\mathbf{B = g^b \bmod p}$ $B = 5^{\mathbf{15}} \bmod 23$
- B = **30,517,578,125** mod 23
- B = 19
- Alice computes **s** = $B^{\,a} \bmod p$ $\quad$ **s** = $19^{\mathbf{6}} \bmod 23$
- **s** = **47,045,881** mod 23
- **s** = **2**
- Bob computes **s** = $A^{\,b} \bmod p$ **s** = $8^{\mathbf{15}} \bmod 23$
- **s** = **35,184,372,088,832** mod 23
- **s** = **2**

Problem…

- Man in the middle attack……Eve simply pick up the value of ‘n’ & ‘g’.
- Alice & Bob select their random number x,y and compute X & Y. Eve also select new random numbers and compute X & Y…….
- Alice sends her ‘x’ to Bob. Eve intercepts it and instead given his ‘x’ to Bob…In return bob sends his ‘y’ to Alice, Eve intercepts it and sends his ‘y’ to Alice.