**Key Agreement**

Asymmetric key cryptography is more complex and slower than symmetric, but

* Key management is simplified (only 1 party needs to know the private key, knowledge of public key does not compromise the security of message transmissions)
* Key distribution is scalable (each subject has one key-pair (pvt and public).

Keys in symmetric= n(n-1)/2

Keys in asymmetric=2n

* Key establishment can be authenticated (pvt and public key are mathematically related

DH algorithm: (Y^x mod P, find x where Y^x = Z (mod P)

**Peer-to-Peer key distribution**: technically easy (Distribute shared keys to each entity we want to communicate with), does not scale (Hundreds if servers, times thousands of users, yields million keys)

**Symmetric key crypto problem:** It lets two parties exchange secret messages if they already have a shared key. “How key will be shared”

**Diffie-Hellman Key Exchange: (**Diffie-Hellman key agreement protocol): no need for any prior secret agreement to communicate securely

Diagram

Description automatically generated

**DH in Math-** The mathematics of DH is based on modulo exponentiation+ makes use of big prime numbers. Security relies on difficulty of computing discrete logarithm problem. No efficient algorithm known. Can only be solved through trial and error.

Table

Description automatically generated

Man in the middle attack

A picture containing diagram

Description automatically generated

Elliptic curve algorithm (Asymmetric key cryptography)

Uses algebraic system defined on points of elliptic curve to provide public-key cryptography.

Advantages: Highest strength/bit, fast encryption, and signature speed, small signatures and certificates