Recall that there are two basic types of encryption:
symmetric algorithms: (also called “secret key”) use the same key for both encryption and decryption;
asymmetric algorithms: (also called “public key”) use different keys for encryption and decryption.

For any encryption approach, there are two major challenges:
Key distribution: how do we convey keys to those who need them to establish secure communication.
Key management: given a large number of keys, how do we preserve their safety and make them available as needed.

Asymmetric Encryption Primer

In asymmetric or public key encryption, different keys are used for encryption and decryption.

Each subject $S$ has a publicly disclosed key $K_S$ (“$S$’s public key”) that anyone can use to encrypt, and a privately held key $K_S^{-1}$ (“$S$’s private key”). The relationship is:

$$M = \{\{M\}_{K_S}\}_{K_S^{-1}}.$$

Anyone wishing to send a message $M$ confidentially to $S$ sends $\{M\}_{K_S}$. Only the holder of $K_S^{-1}$ can decrypt this message.

Asymmetric encryption largely solves the key distribution problem. Why?

How Many Keys: Symmetric Encryption

Given a symmetric system with $n$ users, how many keys are needed for pairwise secure communication?

Each time a new user is added to the system, it needs to share a new key with each previous user. Thus, for $n$ users, we have

$$1 + 2 + \ldots + (n - 1) = n(n - 1)/2$$

This is $O(n^2)$ keys.
Given an asymmetric system of \( n \) users, how many keys are needed for pairwise secure communication?

Each time a new user is added to the system, it needs only a public key and a private key.

Thus, for \( n \) users, we have \( 2n \) keys, which is \( O(n) \).

Depending on the algorithm, each user may need separate pairs for confidentiality and signing, i.e., \( 4n \) keys, which is still \( O(n) \).

Typically, in a symmetric encryption system keys are:
- randomly generated \( k \)-bit strings,
- simple to generate,
- have no special properties.

In a public key system, keys:
- have special structure (e.g., are large primes), and
- are expensive to generate.

Key sizes are not comparable between the two approaches. A 128-bit symmetric key may be equivalent in strength to a 3000-bit public key.

Using symmetric encryption, security requires that each pair of users share a secret key.

In an asymmetric system, each user has a public/private key pair.

Keys in the two approaches have very different characteristics and are not directly comparable.

Next lecture: Stream and Block Encryption