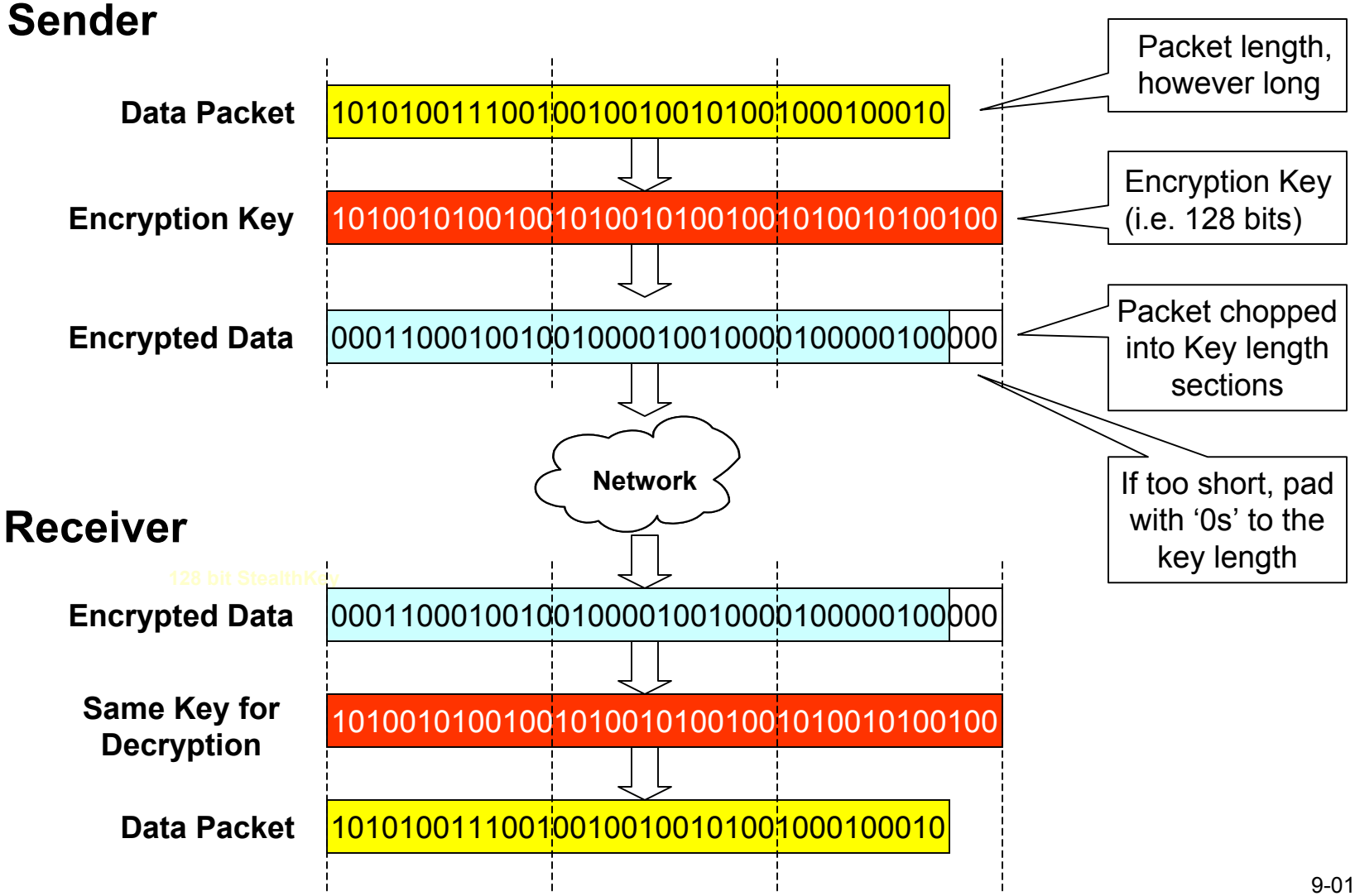
Encryption Fundamentals

Hugo Fruehauf
hxf@zyfer.com
October 2001

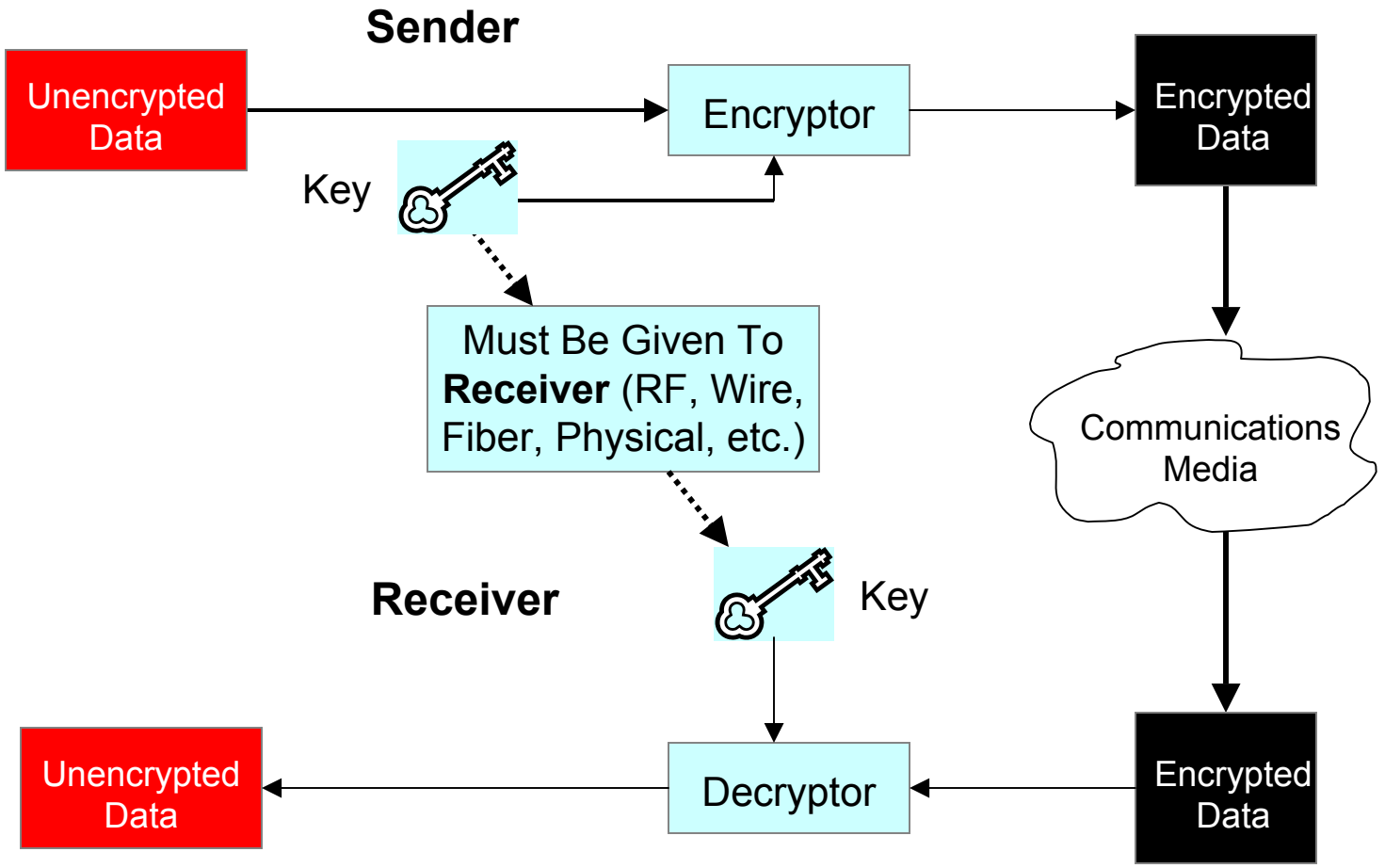
Securing Data through a Cryptographic Process



Cryptographic Algorithms

- Cryptography allows two parties to exchange sensitive information in a secure manner.
- Encryption scrambles the information so that only the intended recipient can recover the original information by decrypting it.
- Two types of cryptographic algorithms
  - *Symmetric (Secret-Key) algorithms*
  - *Asymmetric (Public-Key) algorithms*
- Cryptography can also provide the following security properties
  - Authentication - authenticates the party that sent the information.
  - Integrity - assures that the information was not modified while in transit.
  - Non-repudiation - disallows a party denying a previous message or action.

Symmetric (Secret-Key) Cryptography



Symmetric Key Pros and Cons

- Pros:
  - Fast
  - Easy to implement in hardware
  - Widely used
- Cons:
  - Secret key must be exchanged via a trusted (secure) channel
  - Most have fixed key length
  - Can be intercepted if poor algorithm is used
  - Requires added effort for authentication of sender
  - Key administration logistics

A new key must be created and kept for every new party that exchanges information:

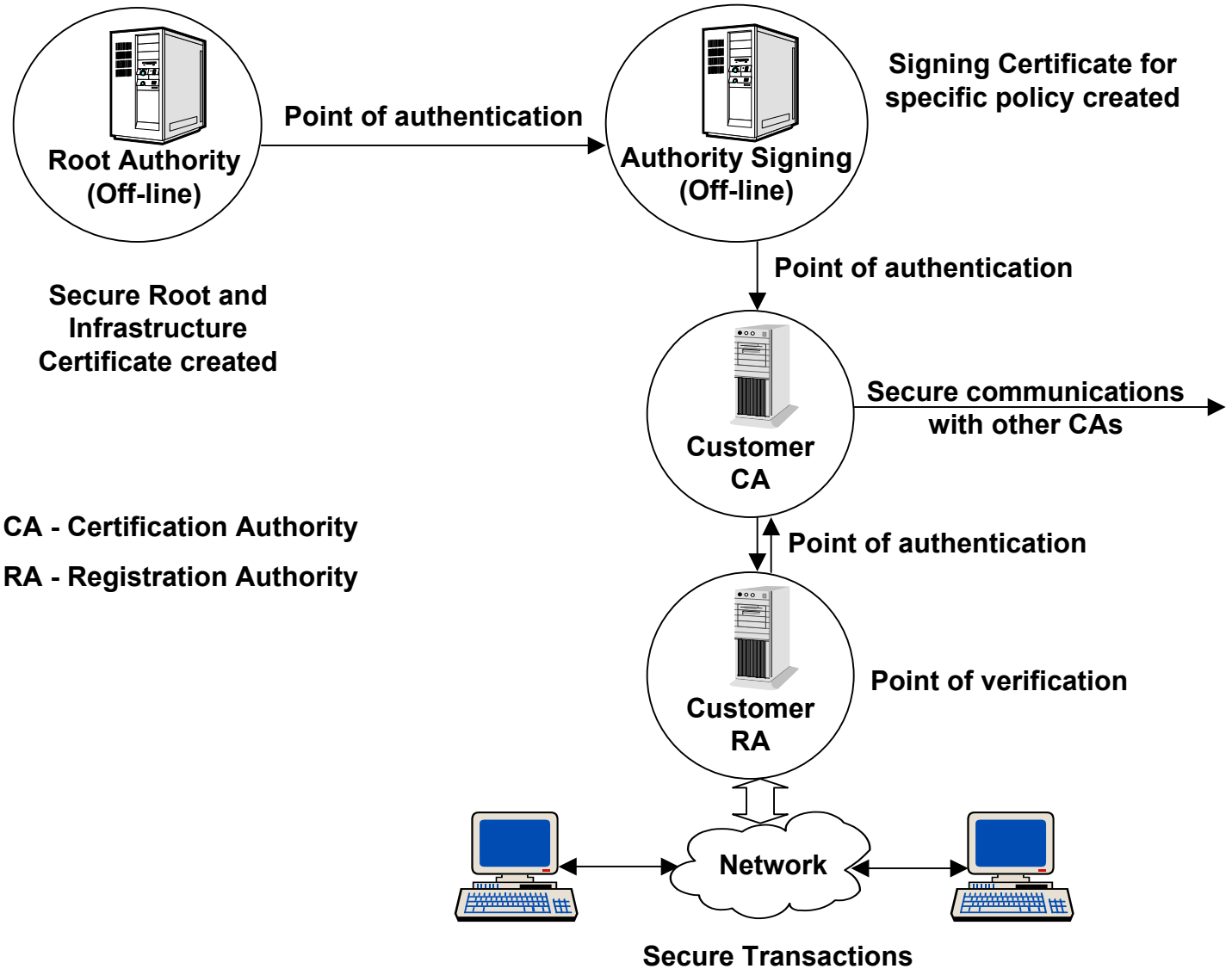
- 2 parties = 1 key
- 3 parties = 3 keys
- 4 parties = 6 keys
- 5 parties = 10 keys

$$\left[\frac{n2 - n}{2}\right]$$

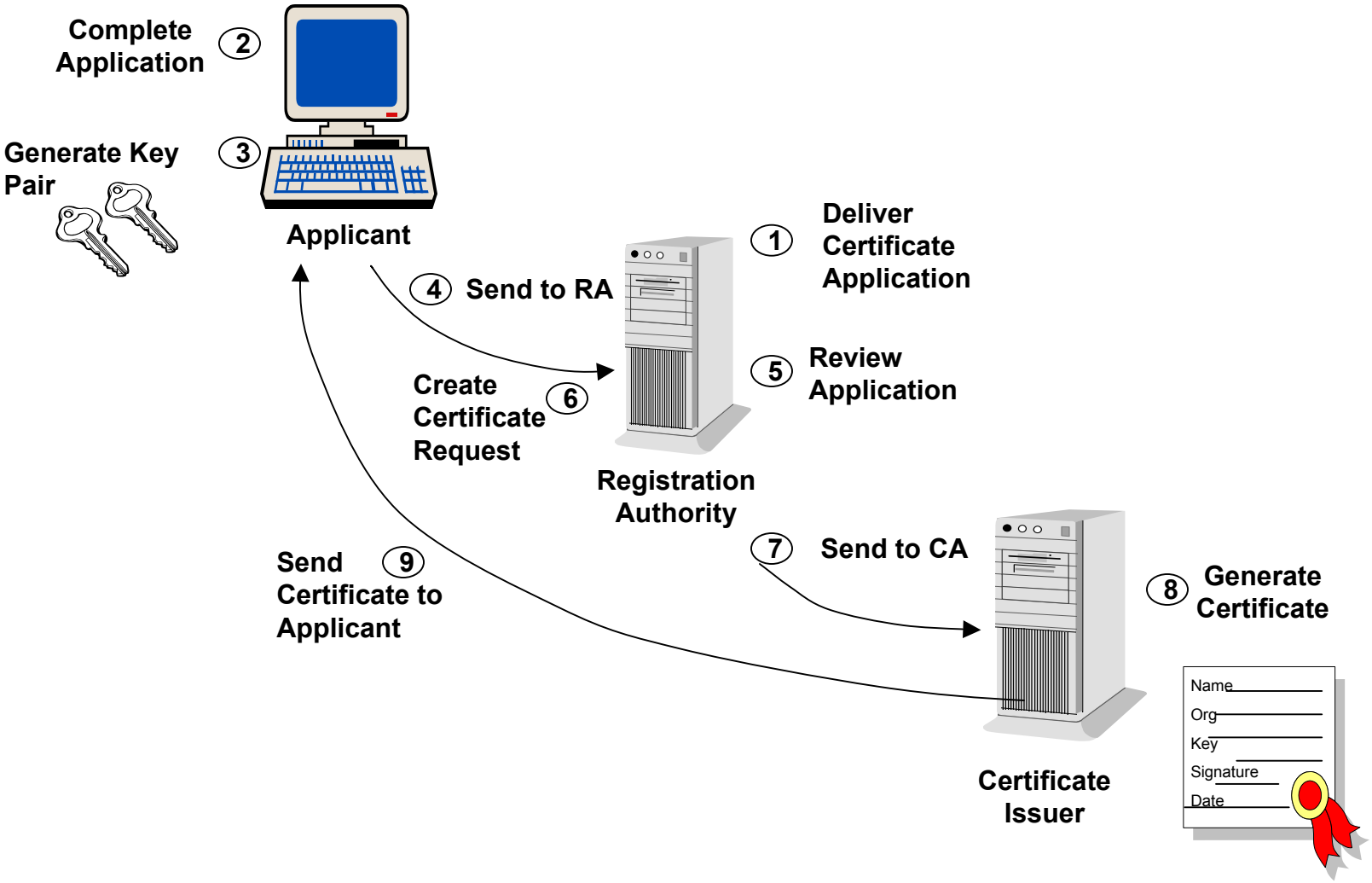
Asymmetric (Public-Key) Cryptography

- Public Key Infrastructure (PKI) definition
  - A policy for establishing a secure method for exchanging information within an organization, an industry or a nation. It includes the cryptographic methods, the use of digital signatures, digital certificates and certification authorities (CAs) and the system for managing the process.
- Provides enterprise-wide security and authentication
- Administers security once for all network applications across all platforms
- Provides security consistently
- Builds a “trusted” network environment

Hierarchical PKI Model

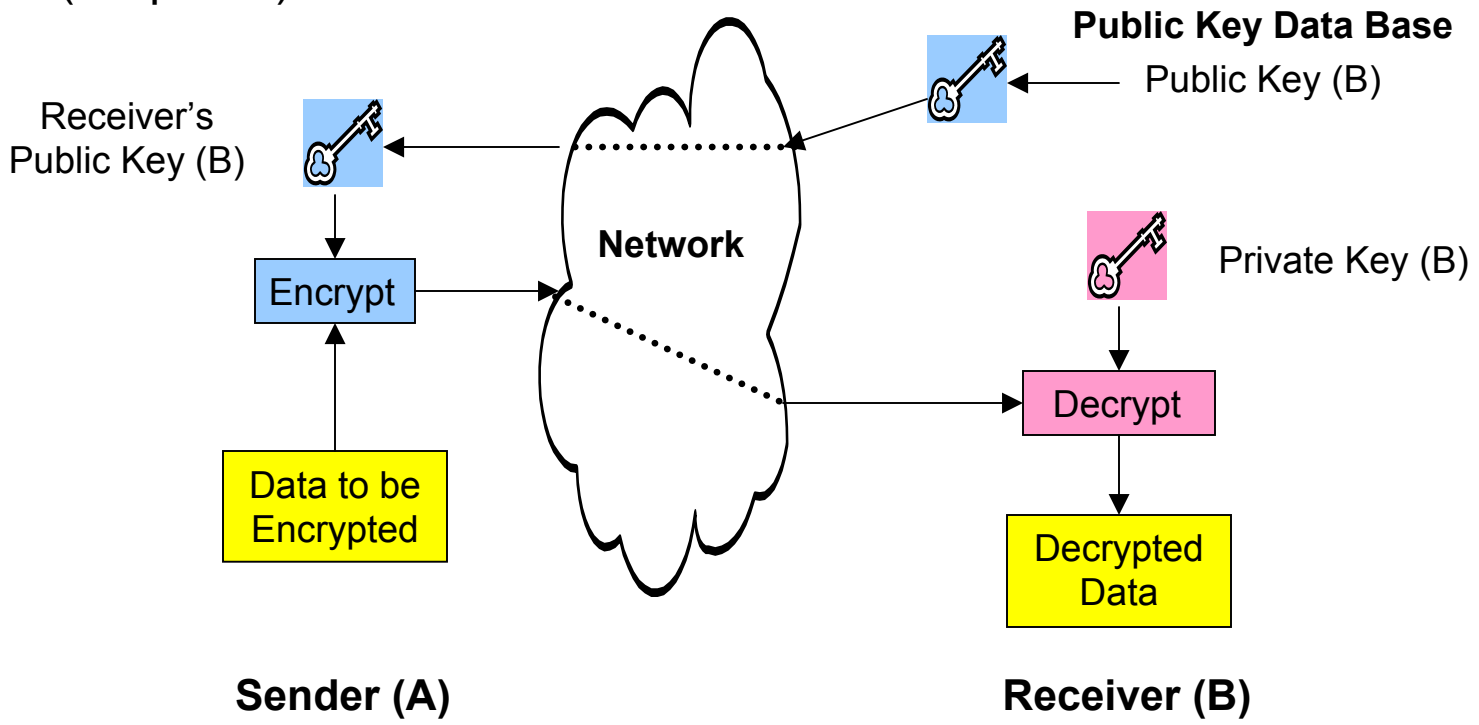


Registration and Certification Process



Basics of Asymmetric (Public-Key) Cryptography

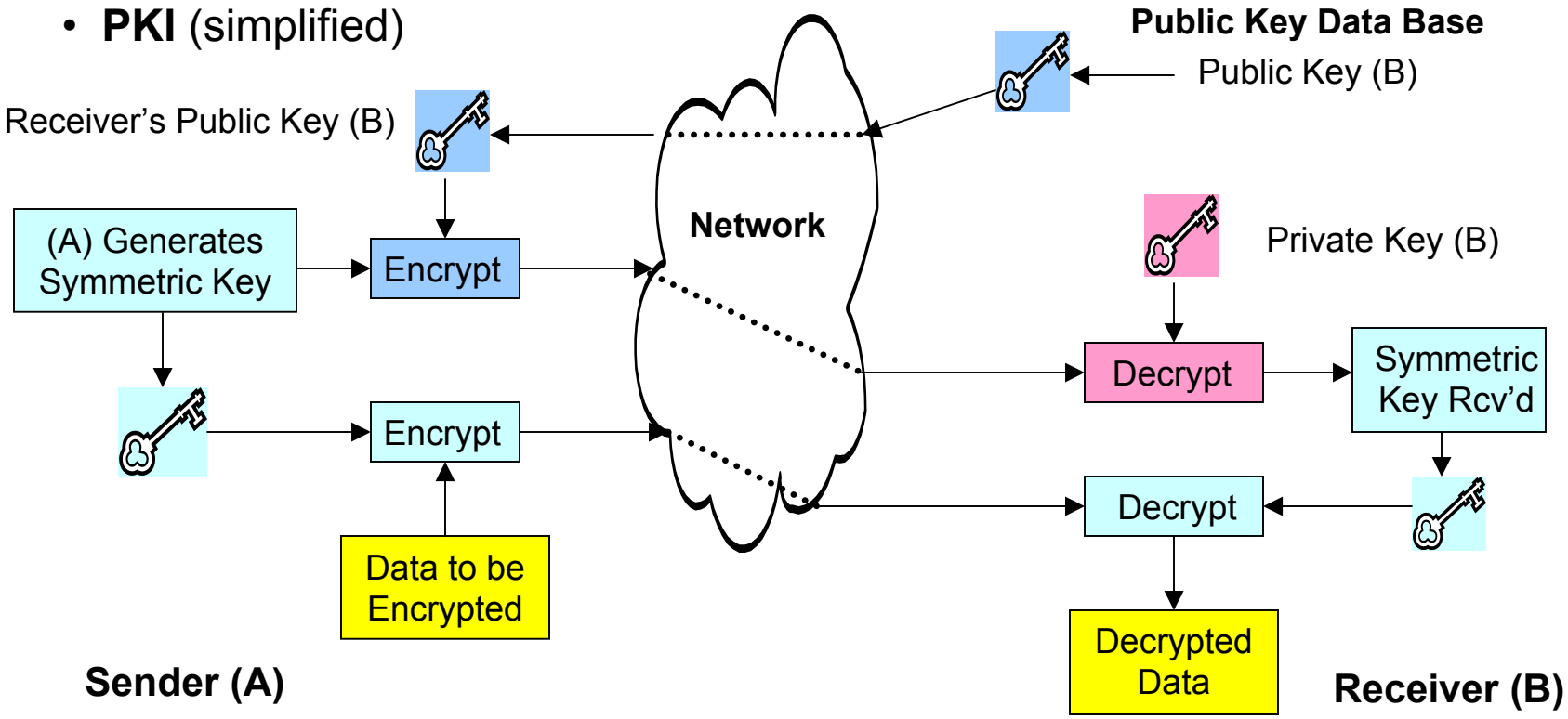
- **PKI** (simplified)



- **Usable mainly for relatively low data rates because asymmetric cryptography is math intensive which slows down the pipe**

Symmetric Key Exchange via PKI

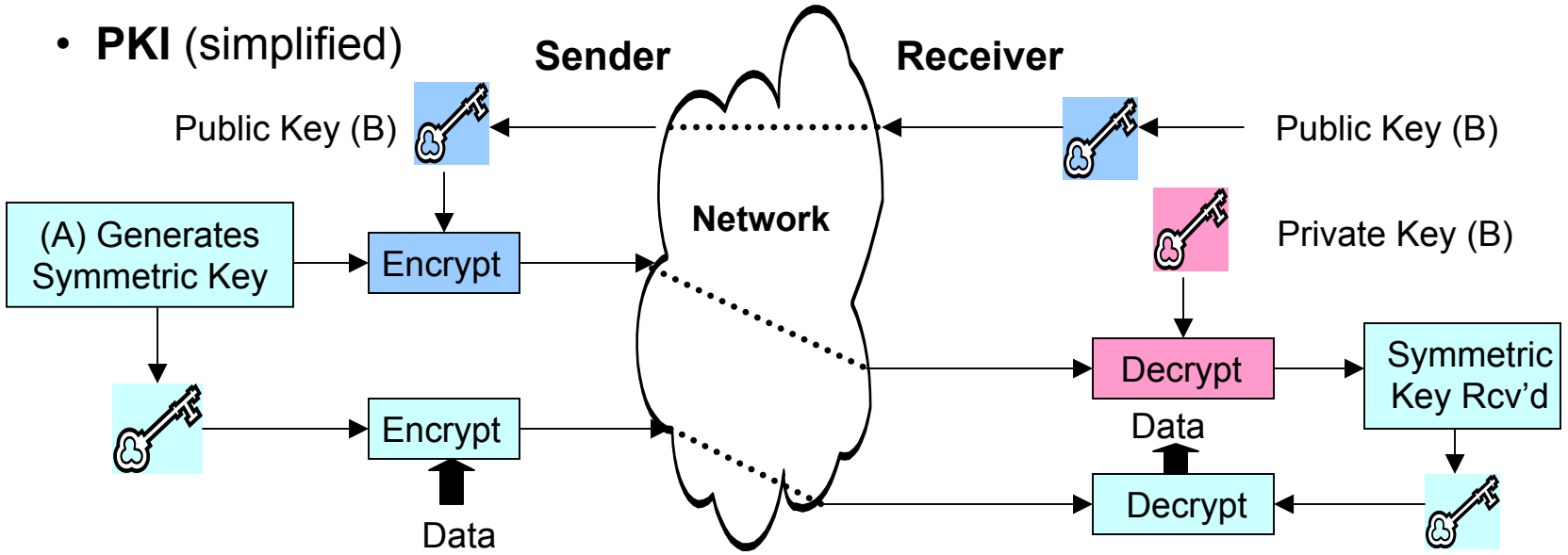
- **PKI** (simplified)



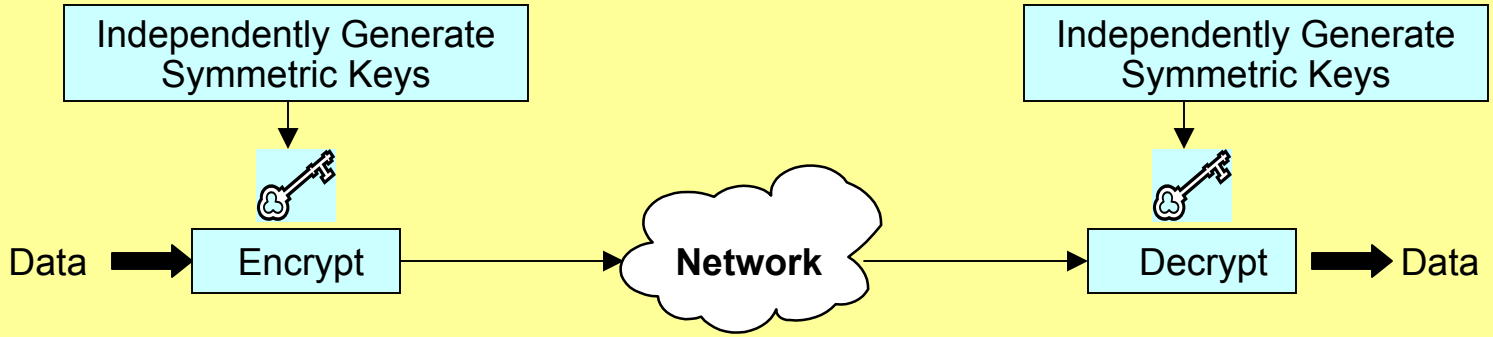
- **Using symmetric key transferred to receiver via PKI, now system is ready for high data rates, no key resolution math, just the encryption algorithm which should not to slow the pipe**

Public-Key vs. StealthKey™ Infrastructure

- **PKI** (simplified)



- Simplified **StealthKey™** for comparison



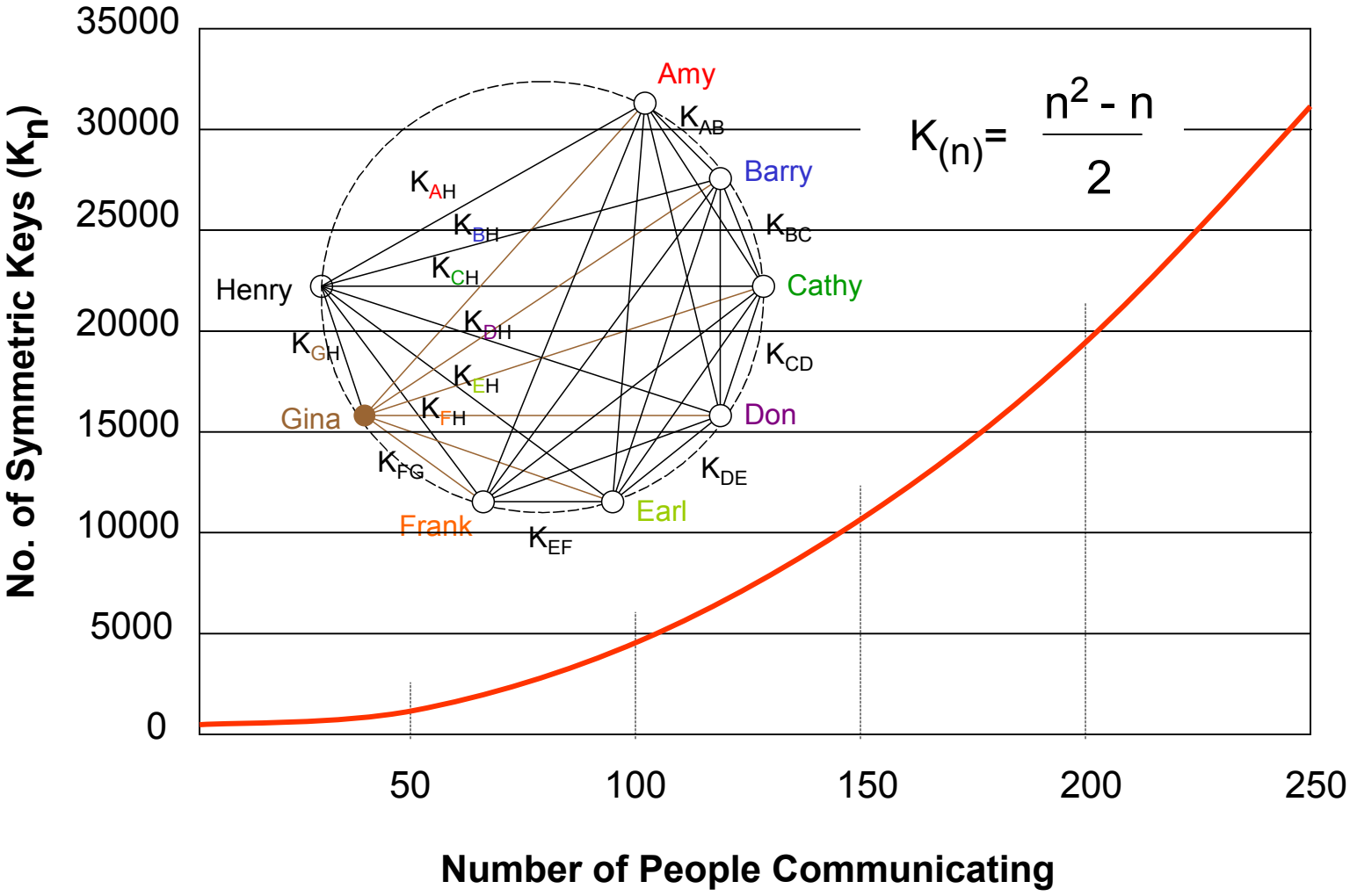
Key Management - The n^2 Problem

If there are 'n' people communicating, there needs to be $(n^2-n)/2$ keys!

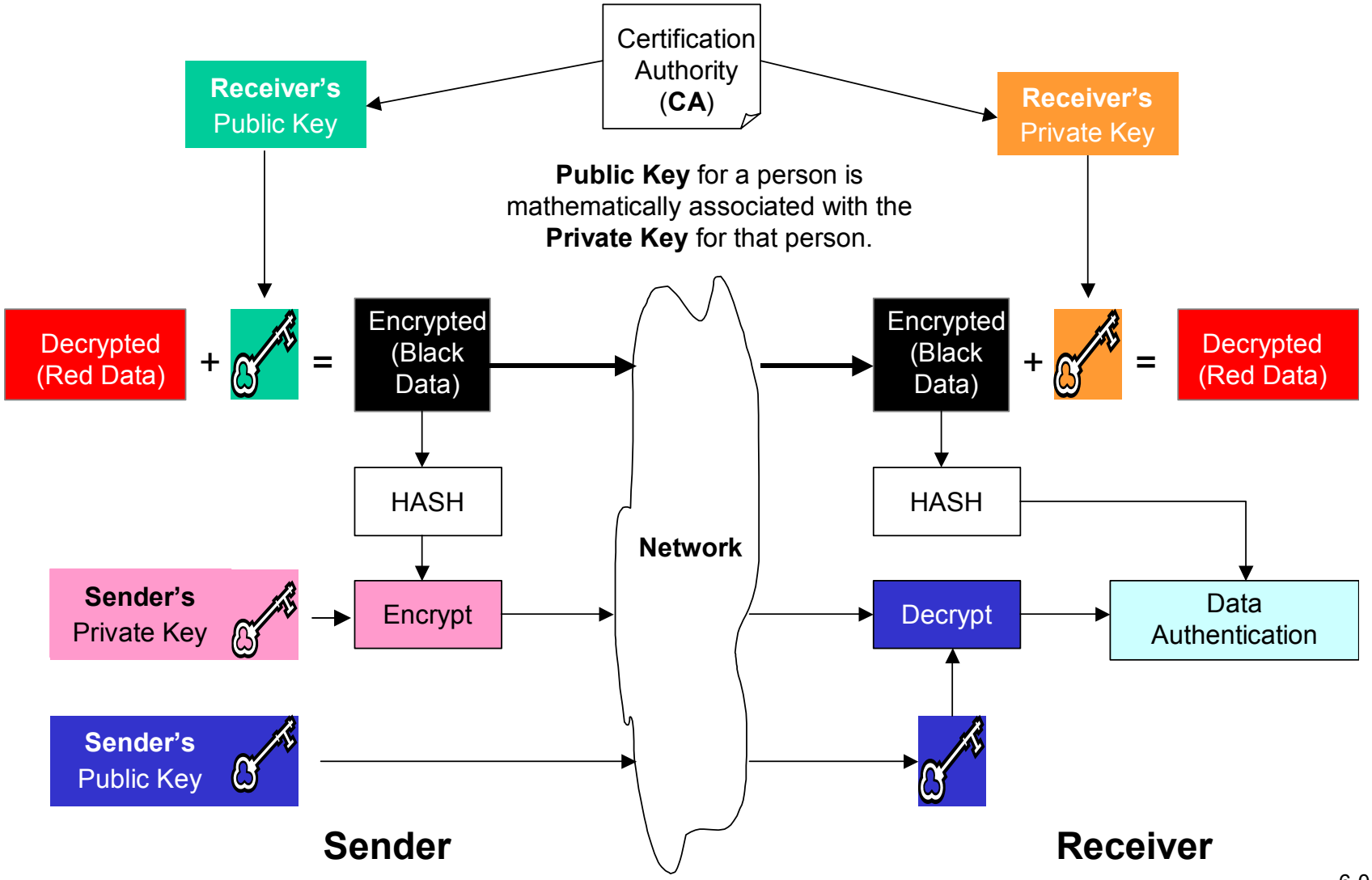
n	$\frac{n^2-n}{2}$						
10	$\frac{10^2-10}{2}$	=	$\frac{100-10}{2}$	=	$\frac{90}{2}$	=	45
100	$\frac{100^2-100}{2}$	=	$\frac{10{,}000-100}{2}$	=	$\frac{9{,}900}{2}$	=	4,950
200	$\frac{200^2-200}{2}$	=	$\frac{40{,}000-200}{2}$	=	$\frac{39{,}800}{2}$	=	19,900

Source: SU and SAIC (modified)

Key Exchange Logistics

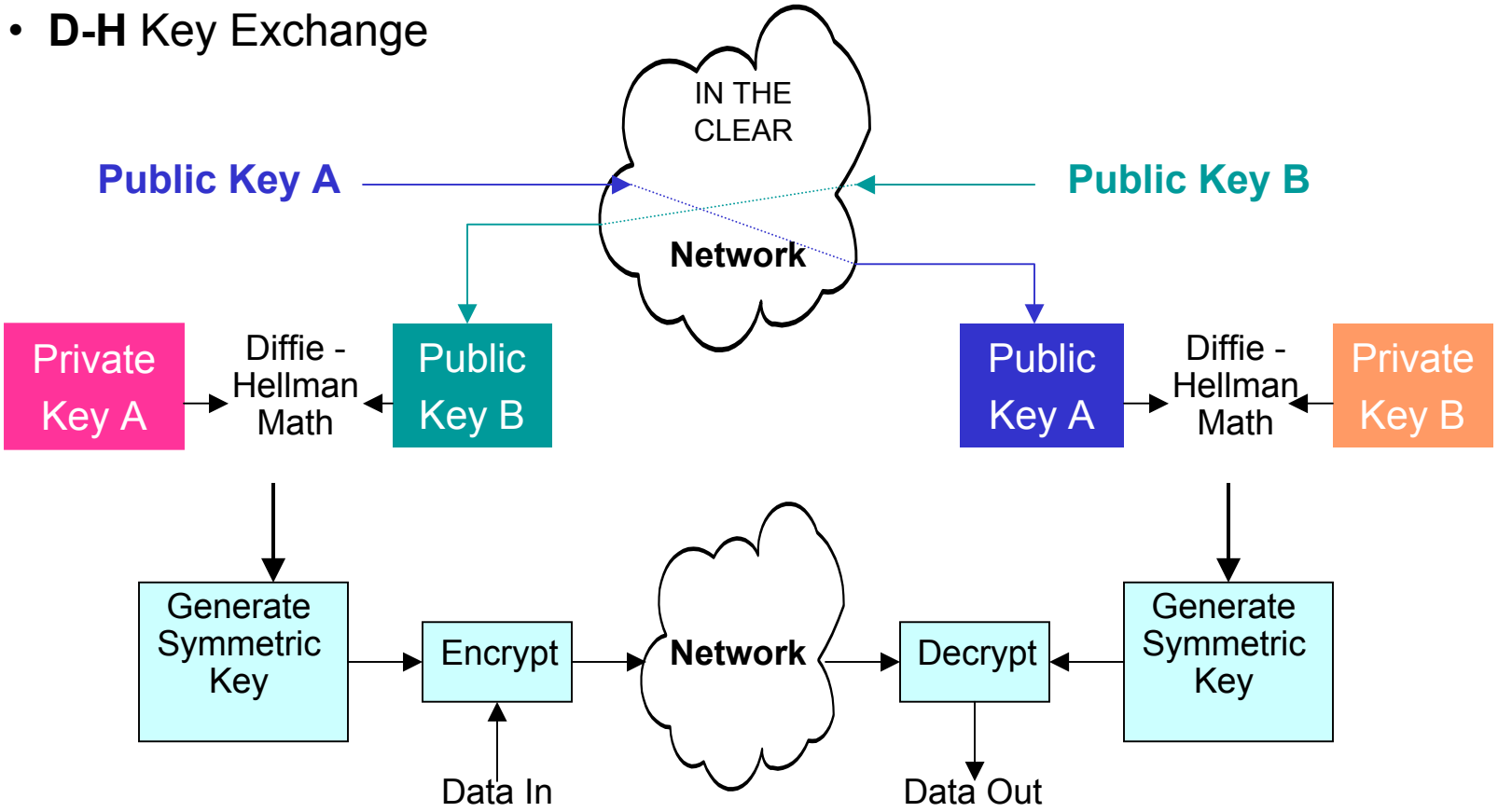


PKI with Data and Sender Authentication

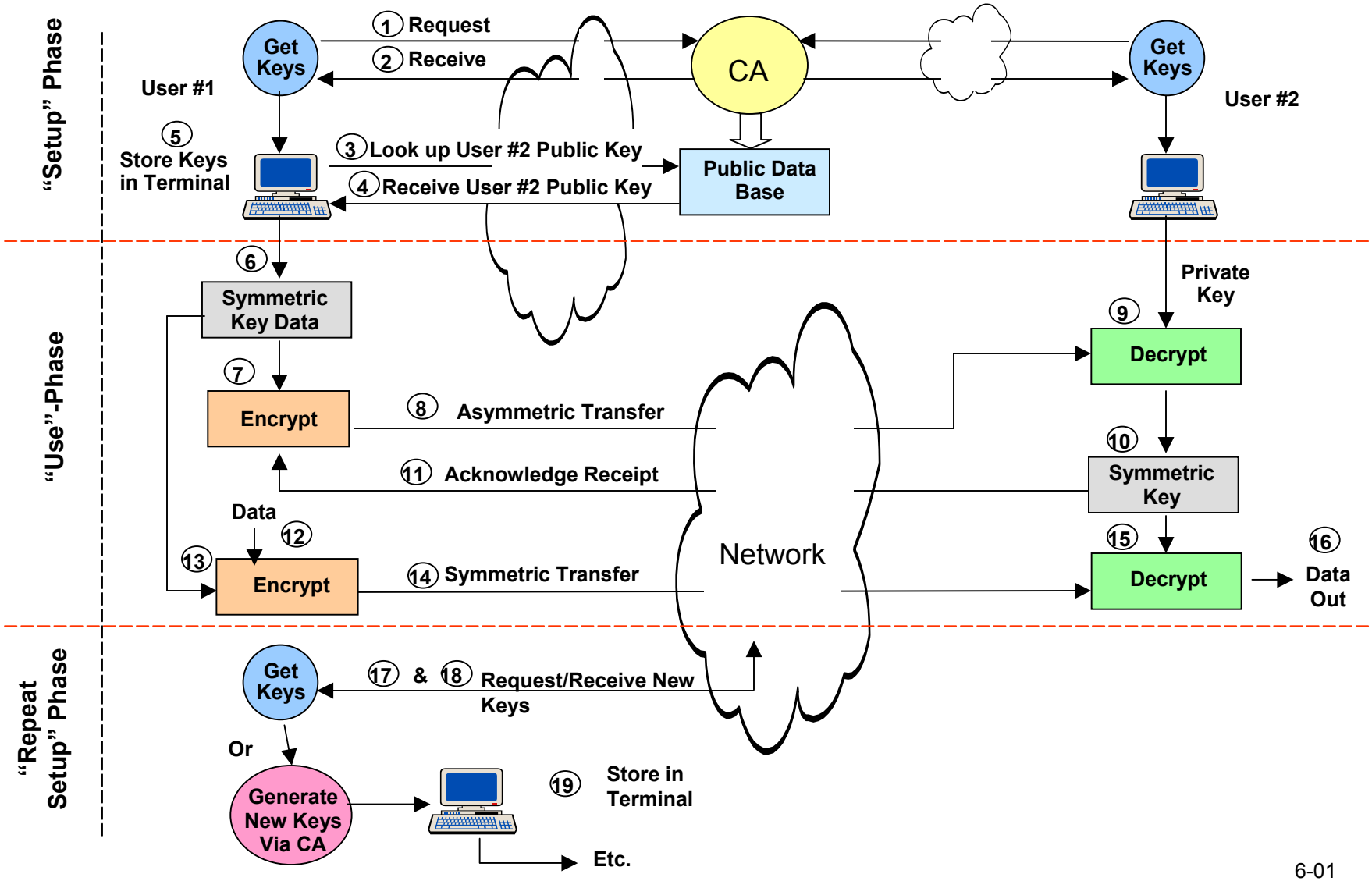


Diffie-Hellman Infrastructure

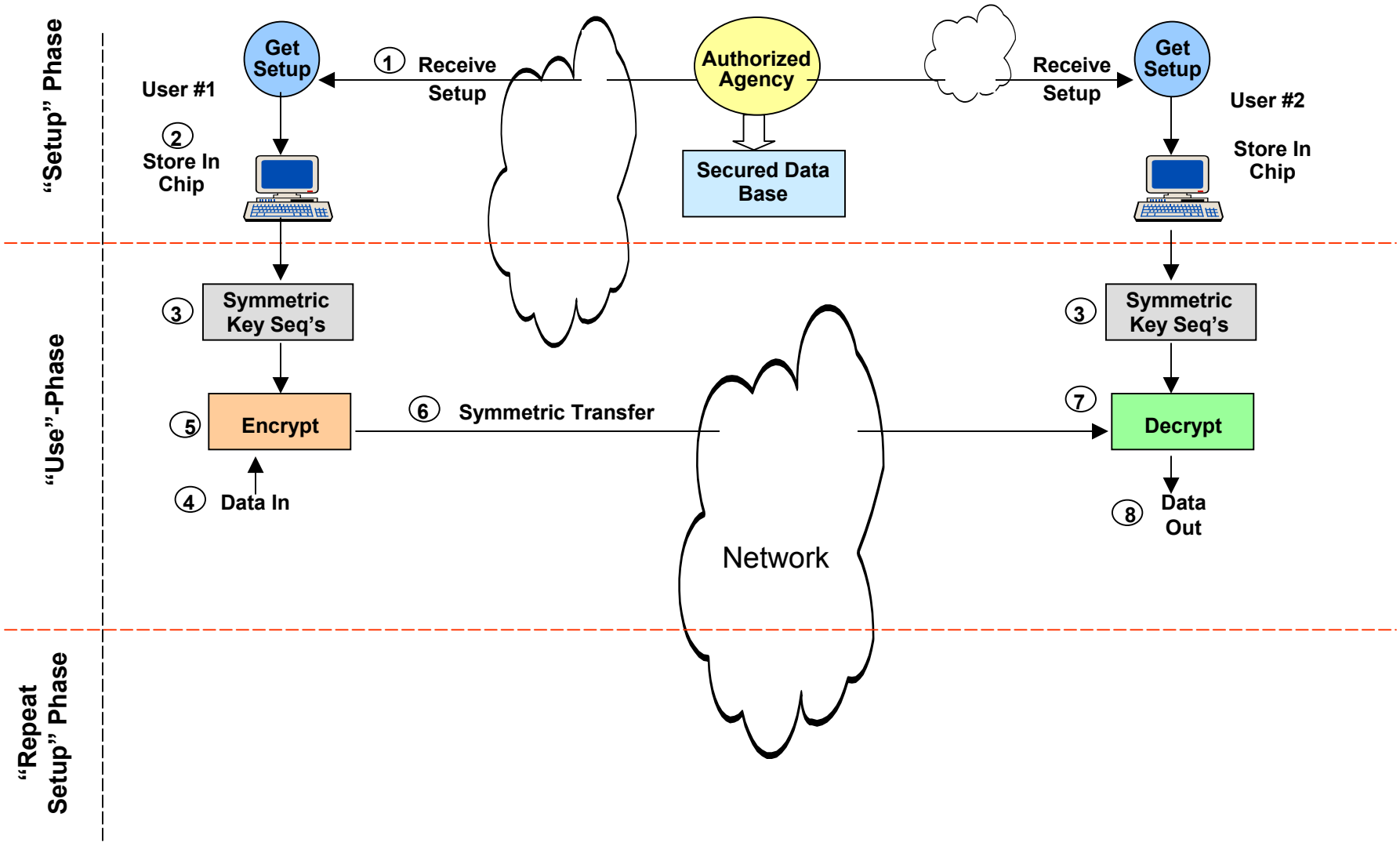
- **D-H** Key Exchange



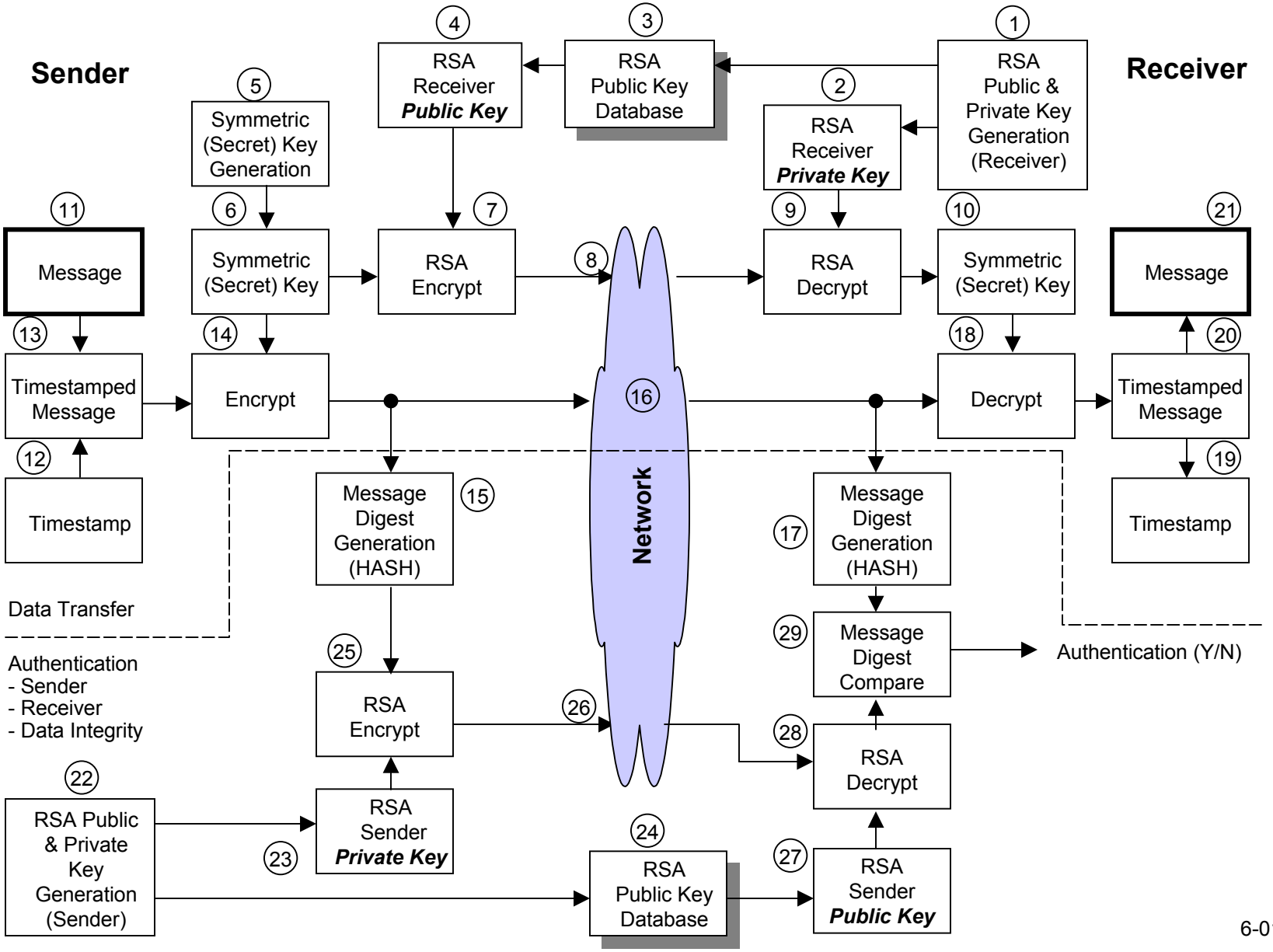
Today's Cryptography Systems (Simplified)



StealthKey™ Cryptography Infrastructure



RSA - Public Key Infrastructure Details



Asymmetric Keys Pros and Cons

- Pros:
  - Does not require a trusted (secure) channel
  - Inherently provides authentication of sender
  - Variable key lengths
- Cons:
  - Computationally intensive, not usable for high speed applications
  - Not easily implemented in hardware
  - Authentication of public keys
  - Key administration logistics
  - Asymmetric algorithms mathematically relate two keys materials - a public and private key pair
  - The public key is in the open domain
  - The private key is protected by a password in a secure location, usually in a PC, smart card or floppy
  - The public key is generally used to encrypt data and the mated private key for decrypting data

Role of Certification Authority

- Certification Authorities (CA) establish the validity of certificates, allowing an identity to be bound to a public key and providing confidence that the binding is valid.
- CAs issue, manage, and revoke certificates for the user communities.
- Certification Authorities
  - Validate identity of certificate subject (to various degrees)
  - Certify certificates with CA digital signature
  - Enforce certificate validity
  - Maintain a certificate revocation list (CRL)
  - Generate Key Pairs

Source: Chokhani, S., Ford, W., "Internet Public Key Infrastructure: Certificate Policy and Certification Practices Framework," IETF Internet Draft, draft-ietf-pkix-ipki-part4-02.txt, 30 September 1997.

Digital Signatures

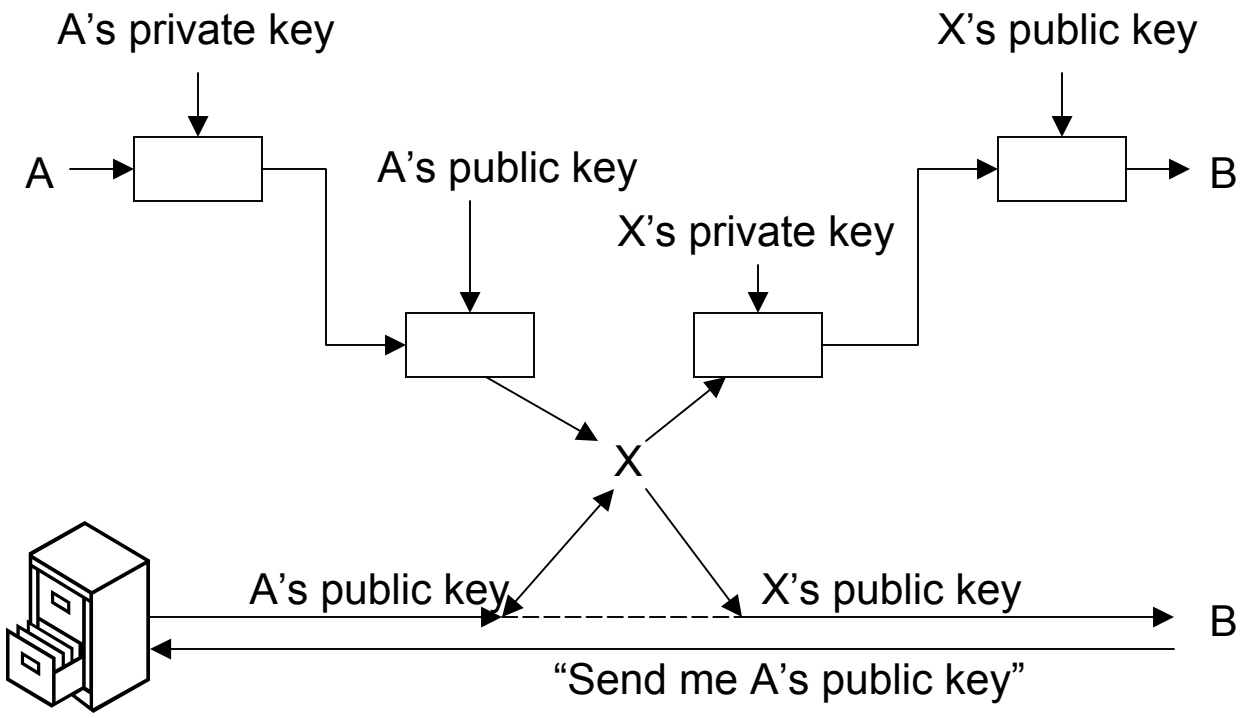
- Digital Signatures:
  - An authentication mechanism that enables the creator to attach a code that acts as a Signature. The signature guarantees the source and integrity of the file.
  - Provides authenticity and integrity.
    - Authenticity or Source: The sender of the information is who he says he is.
    - Integrity: The information sent has not been changed during the transmission.
- Encryption vs. Digital Signatures
  - Encryption solves:
    - Confidentiality
    - Access Control
  - Digital Signature solves:
    - Information Integrity
    - Authentication
    - Non-Repudiation

Digital Signatures

- Creation:
  - Hash the data object to be signed.
  - Encrypt the hash with your private key.
  - Transmit both the data object, public key and the encrypted hash.
- Verification
  - Hash the data object received.
  - Decrypt the encrypted hash with senders public key.
  - Compare the computed hash with the decrypted hash.

Spoofing Attacks

Need for binding A to A's public key



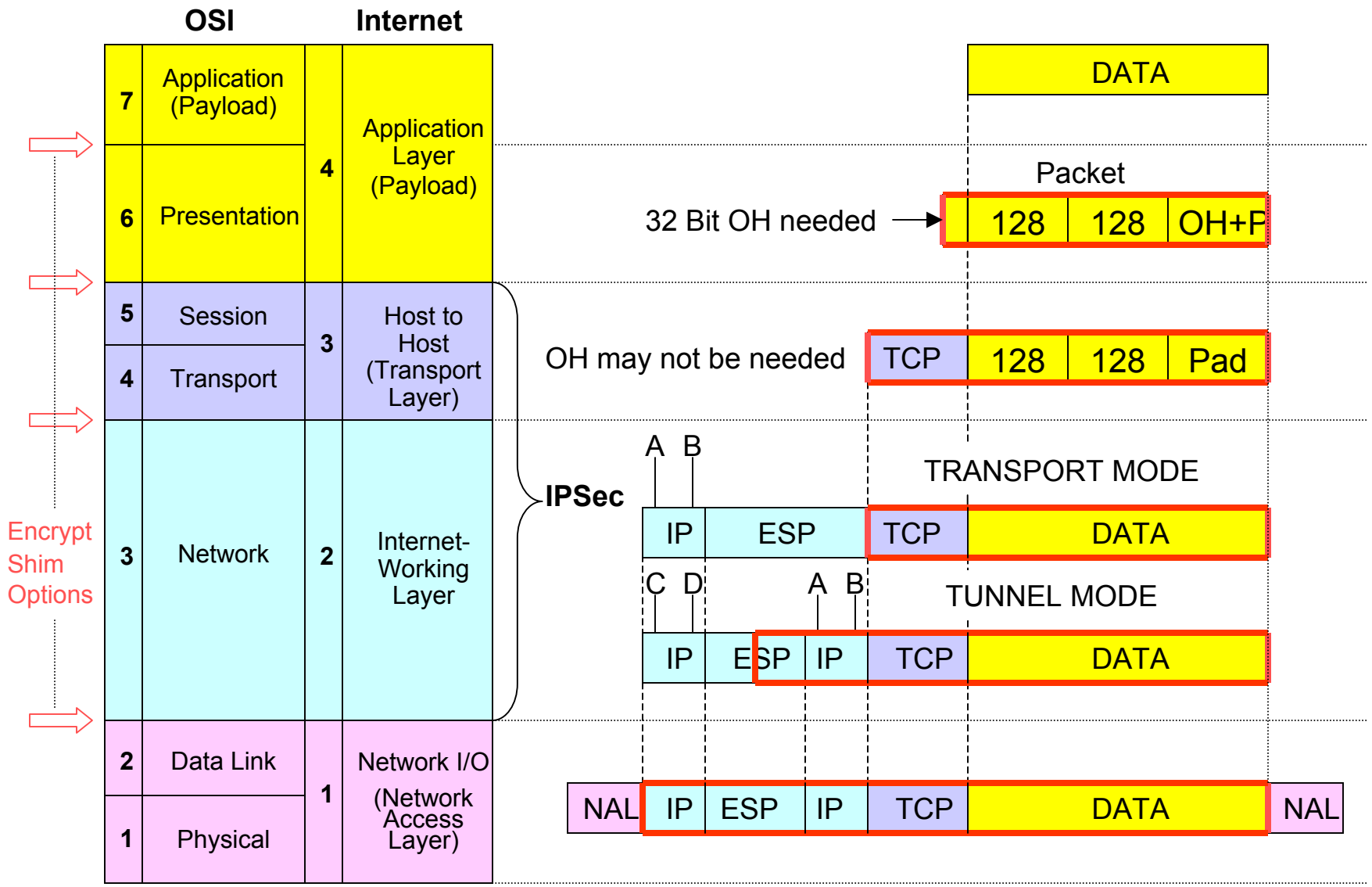
Cost and Time to Break DES Keys

		Time to Break Key		
Type of Attacker	**Budget**	**40-Bit**	**56-Bit**	**168-Bit 3DES**
Individual Hacker	$400	5 Hours	38 Years	Too long
Dedicated Hacker	$10,000	12 Minutes	556 Days 22 Hrs*	10^{19} Years
Intelligence Community	$10 Million	0.02 Sec.	21 Minutes	10^{17} Years

(Source: "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security." Blaze, et.al. 1/96; Schneier B. "Applied Cryptography, Second Edition" John Wiley & Sons, Inc. 1996)

* IPSec, Naganand Doraswamy, Prentice-Hall, 1999

StealthKey™ Encryption Layer Options



Internet Performance