Cryptographic Primitives

Security vulnerabilities could lead to catastrophic consequences.

Security requirements are thus excluding requirements.

Security vulnerabilities are however exposed when system is deliberately attacked

Security analysis & assurance involves identifying valuable assets, determining vulnerabilities and possible attacks, applying and testing security solutions.

Unlike Reliability which improves as time goes by and usage increases, security growth models are not well established.

Suppose A wants to send a message to B remotely

What are the possible vulnerabilities ?

Vulnerabilities	Solutions
Eavesdropping	Encryption
Masquerading	Authentication & Authorization
Message Tempering	Message Digests, Message Authentication Codes, Digital Signatures
Replay	Timestamps and Nonce

Cryptography

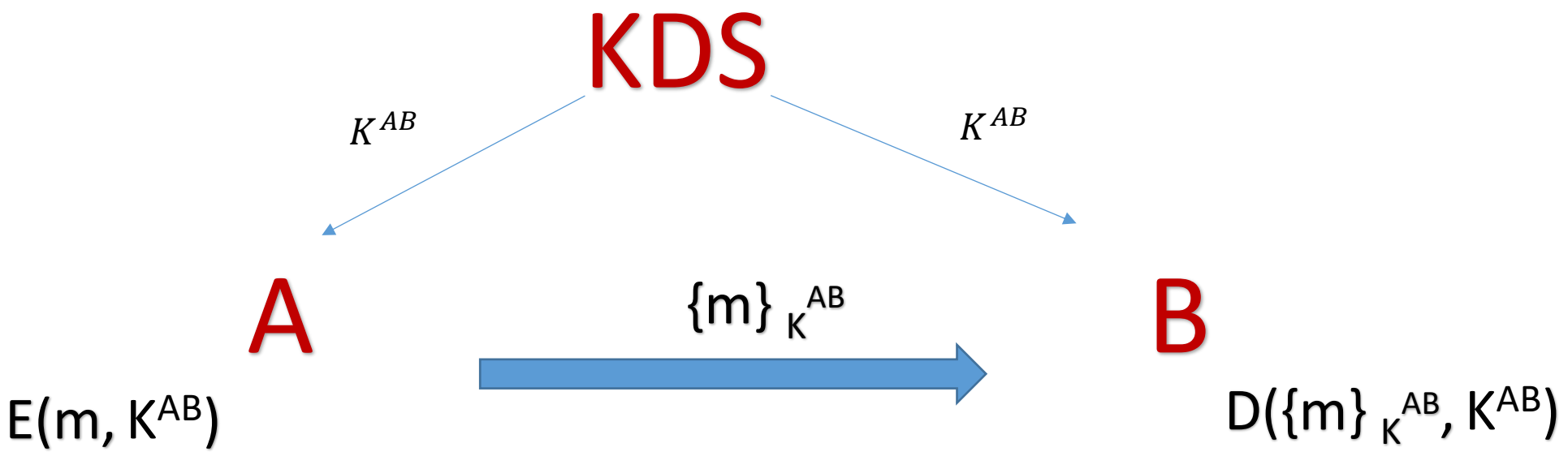
Symmetric

- Stream Ciphers e.g. RC4
- Block Ciphers e.g. AES, DES

Asymmetric

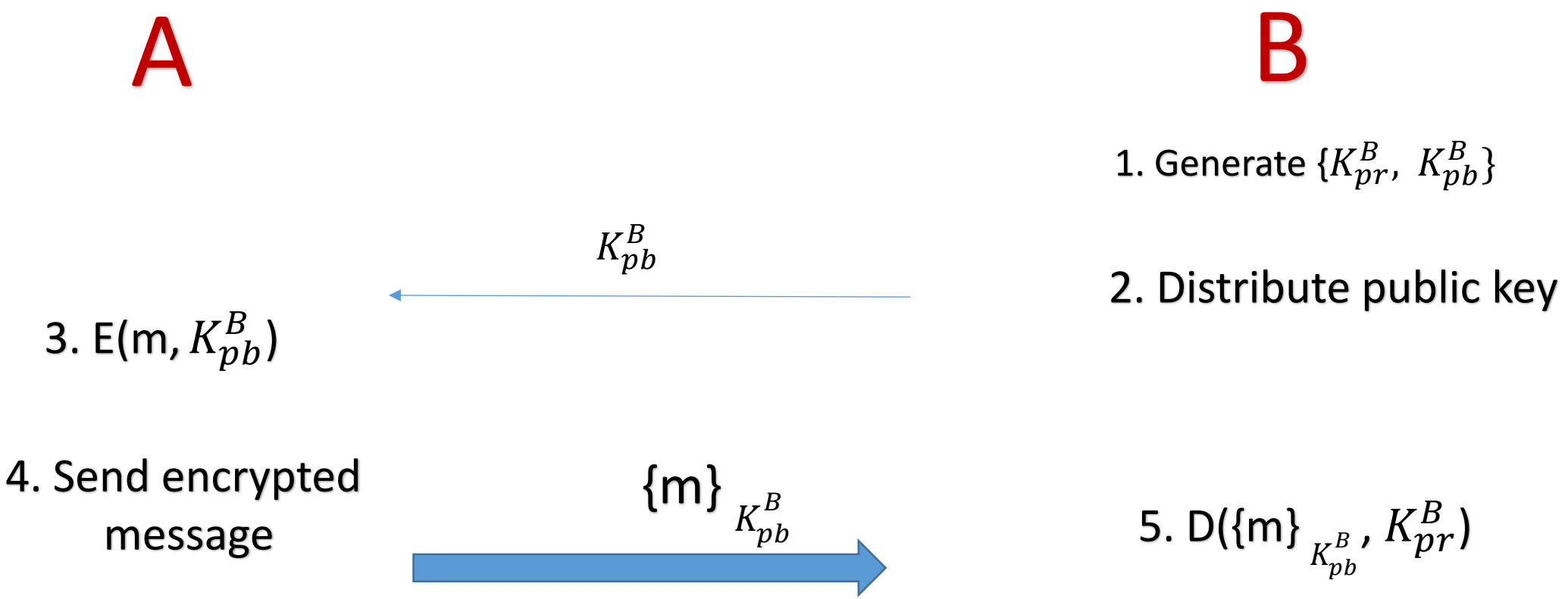
- RSA, Diffi-Hellman and ElGamal

Symmetric Cryptography



- A shared key is used for both encryption and decryption
- E and D are publically known whereas shared key is secret
- Key distribution channels need to be both private and authentic
- Faster

Asymmetric Cryptography



- Public key is used for encryption and private key for decryption
- E, D and the public key are known but private key is secret
- Key distribution channels need to be authentic to prevent man-in-the-middle attack
- cpu intensive

- **Message Digest e.g. MD5, SHA**
  Message digests or Hash functions are used to verify message integrity.

- **Message Authentication Codes e.g. HMAC-MD5, HMAC-SHA**

MAC (Message Authentication Code) is meant to establish the confidence in the recipient that the message was indeed created by the sender.

- **Digital Signatures e.g. X509 certificates**

In addition to verifying the integrity and authenticity like a MAC, a digital signature also protects non-repudiation. The sender of a message creates a digital signature by encrypting the message digest with his/her private key. Non-repudiation is thus guaranteed if the message recipient is able to recover the message digest using the certified public key of the signer.

Security Solutions in Network Stack

Application	**oAuth** • **Authenticates applications to consume user data** **Anti-Spam** • **Filters messages based on content**
Transport	TLS/SSL • Ensures Privacy • Authentication (by default server side but can also authenticate client side) Firewall • Filters packets based on port numbers
Network	VPN e.g. IPSec, PPTP • Ensures Privacy • Authentication of tunnel end points Firewall • Filters packets based on IP address
	802.11x, WPA