

Asymmetric Cryptography

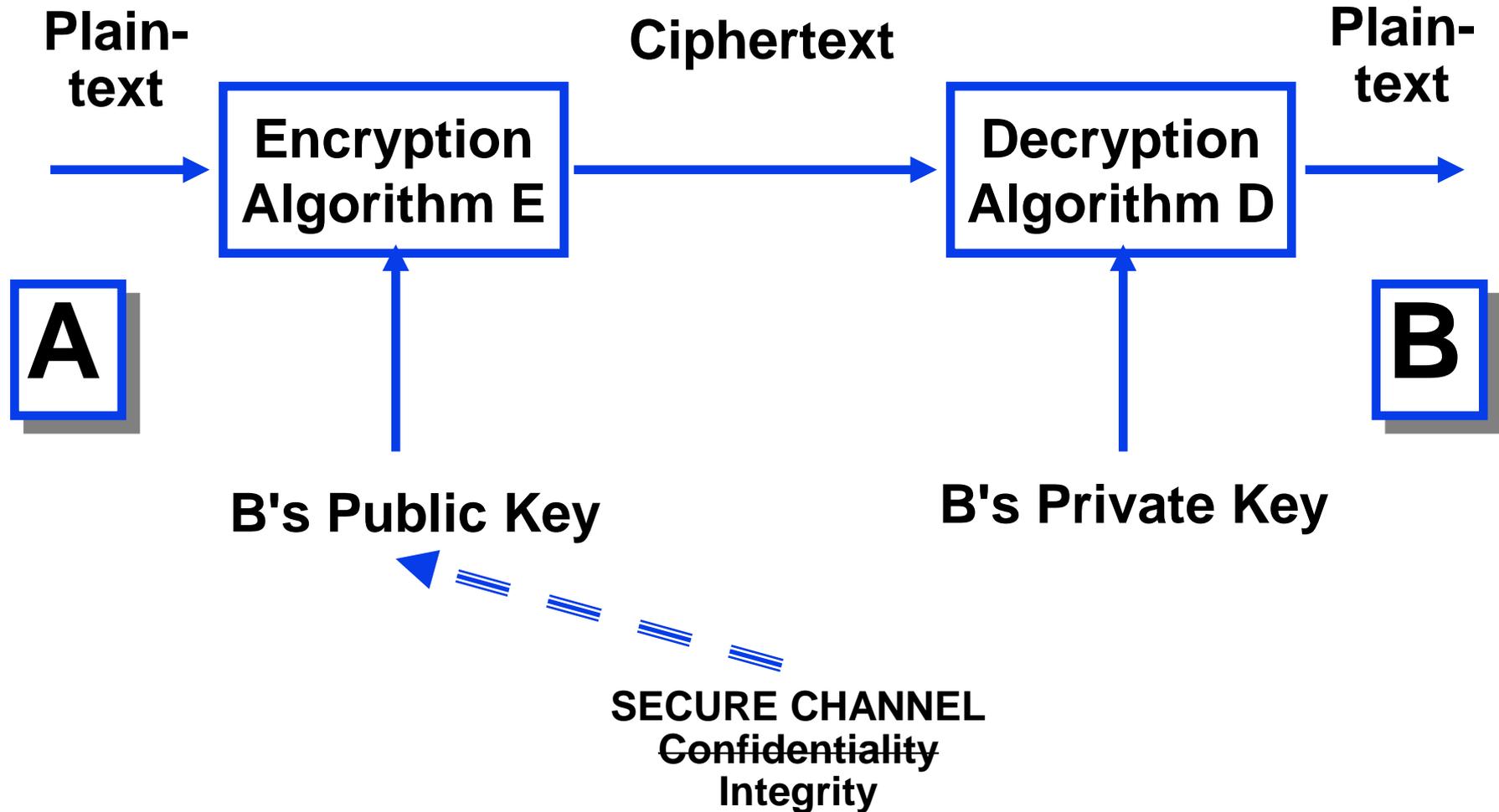
Prof. Ravi Sandhu
Executive Director and Endowed Chair

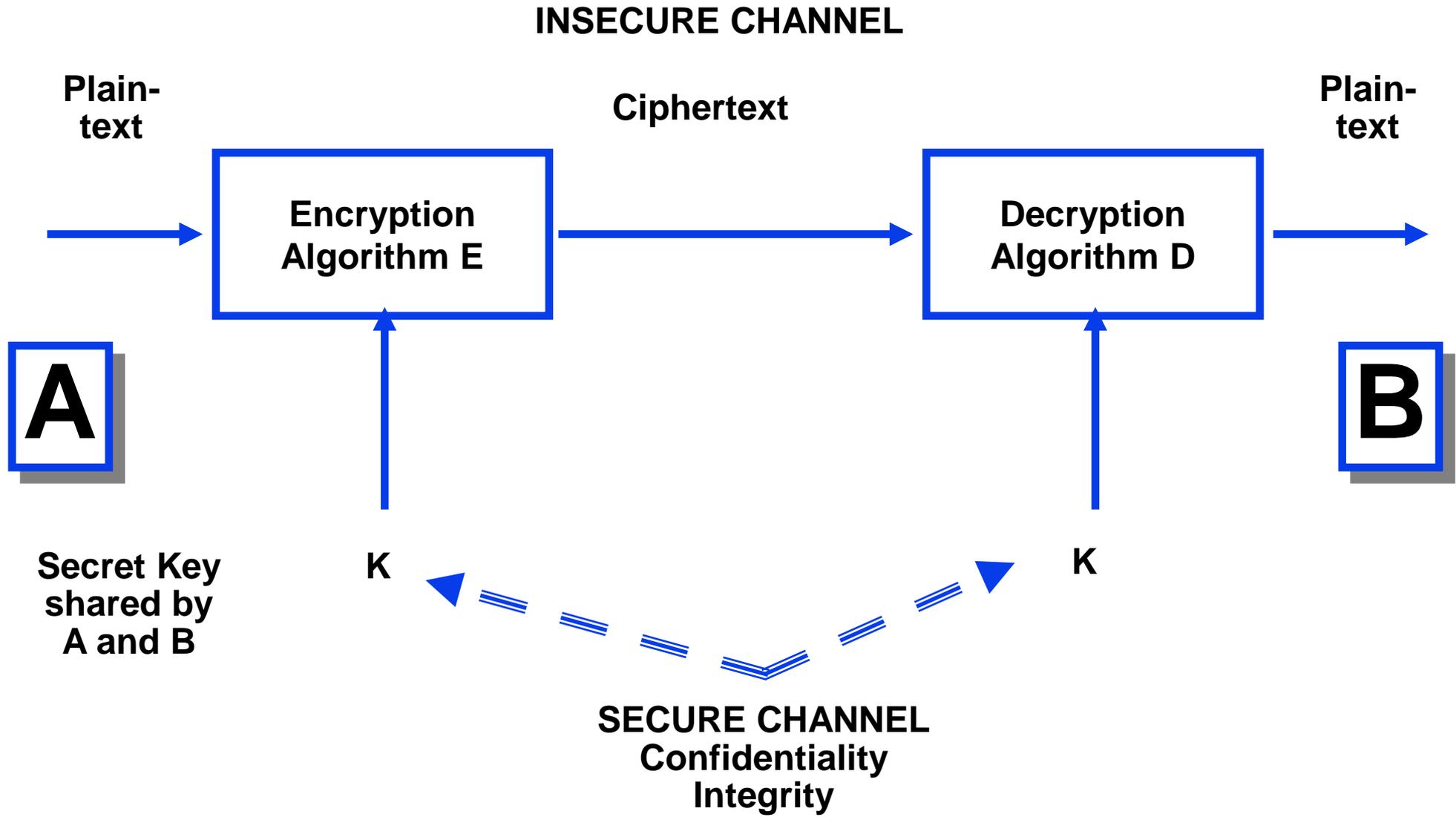
Lecture 8

ravi.utsa@gmail.com
www.profsandhu.com

Asymmetric Encryption

INSECURE CHANNEL





- reduces the key distribution problem to a secure channel for authentic communication of public keys
- requires authentic dissemination of 1 public key/party
- scales well for large-scale systems
 - with N parties we need to generate and distribute N public keys

- confidentiality based on infeasibility of computing B's private key from B's public key
- key sizes are large (2048 bits and above) to make this computation infeasible

- public key runs 1000 times slower than secret key
 - ❖ think 2g versus 4g on smartphone
- This large difference in speed is likely to remain
 - ❖ Maybe reduce to 100 times
- Use public keys to distribute secret keys, use secret keys to protect data

- public key is (n, e)
- private key is d
- encrypt: $C = M^e \pmod n$
- decrypt: $M = C^d \pmod n$

- public key is (n, e)
- private key is d
- encrypt: $C = M^e \bmod n$
- decrypt: $M = C^d \bmod n$

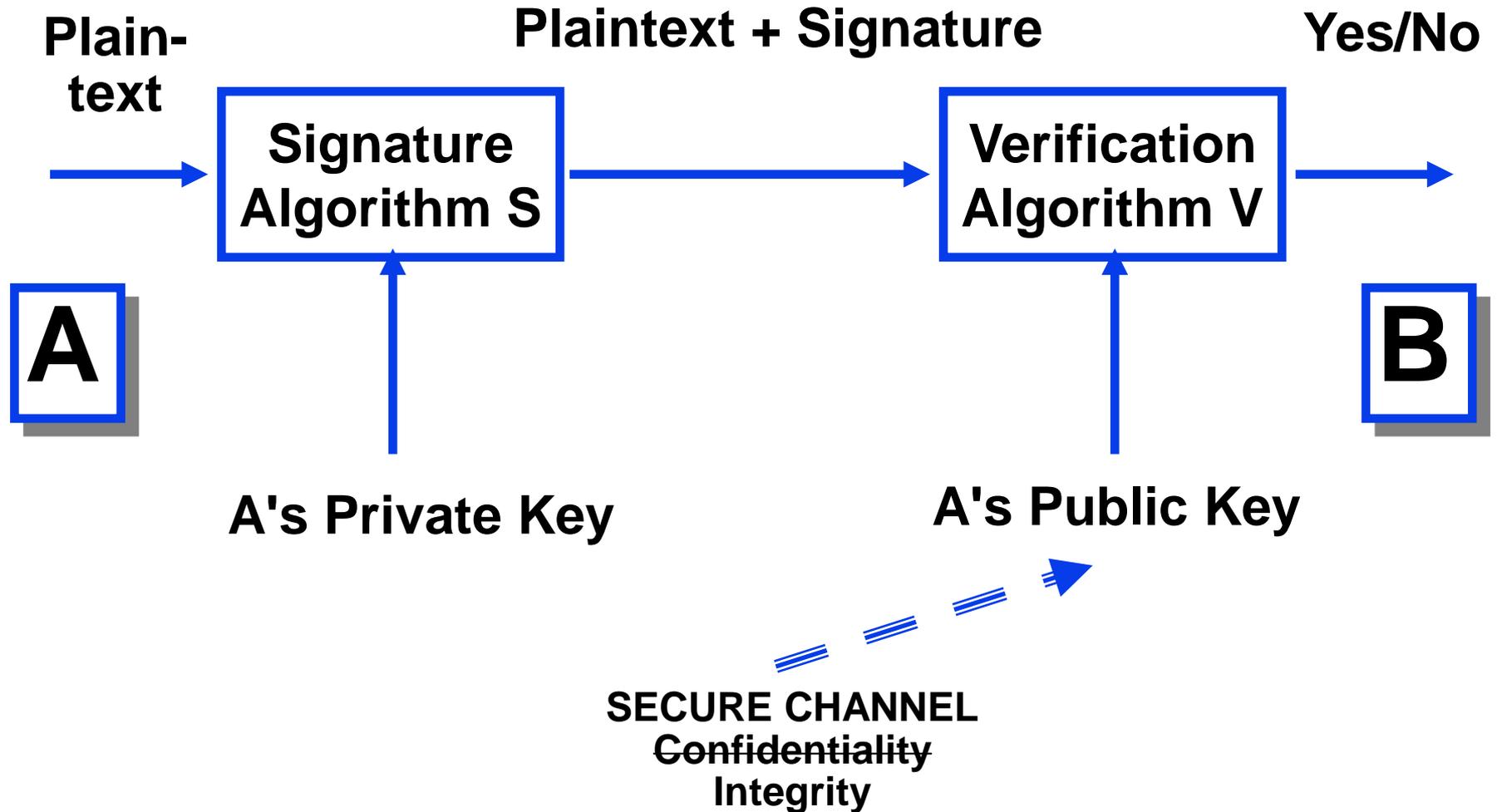
**This naïve use of RSA is
not secure but will
suffice for our purposes**

- choose 2 large prime numbers p and q
- compute $n = p * q$
- pick e relatively prime to $(p-1)*(q-1)$
- compute d , $e*d = 1 \text{ mod } (p-1)*(q-1)$
- publish (n,e)
- keep d private (and discard p, q)

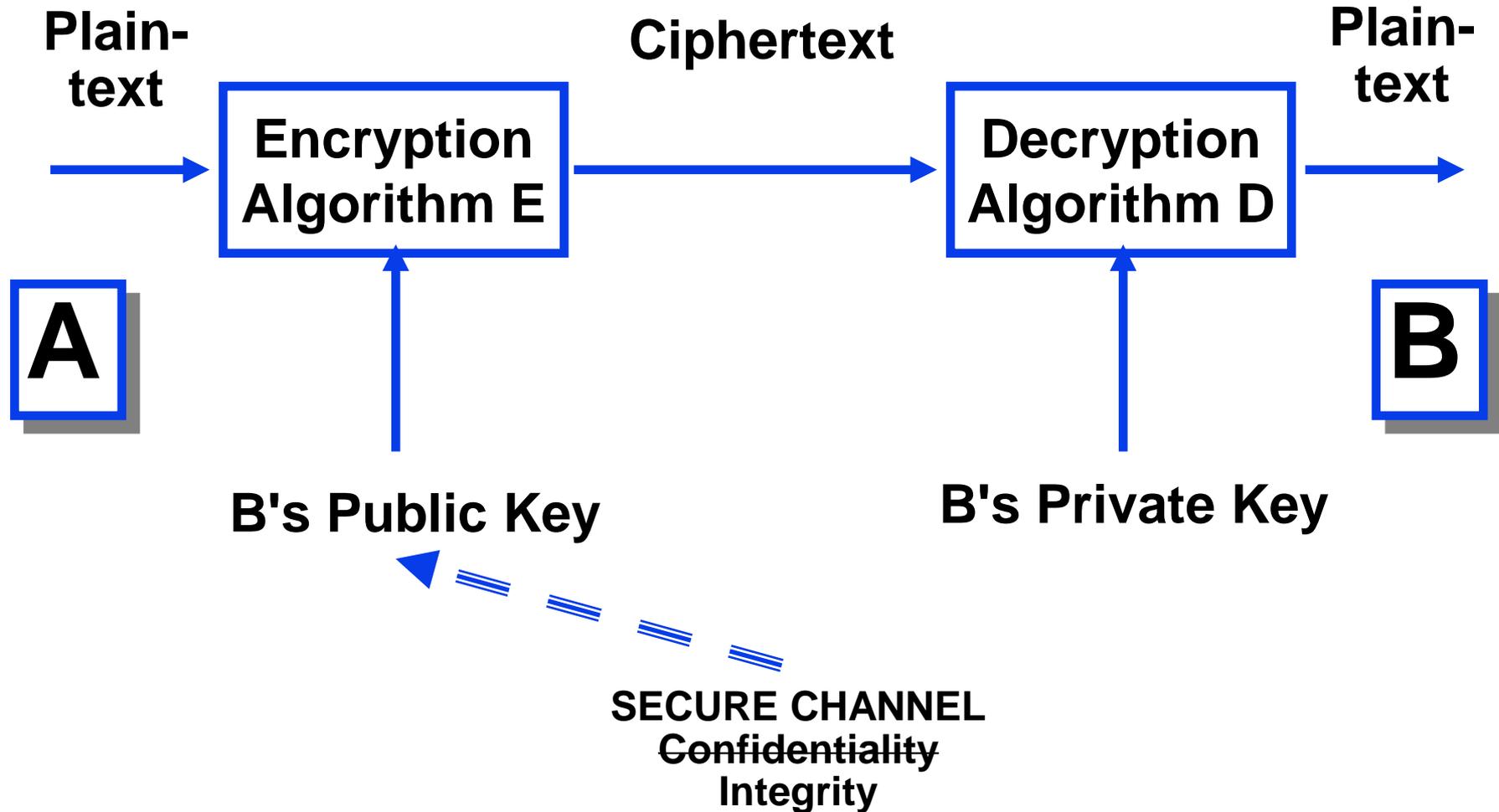
- compute d , $e \cdot d = 1 \pmod{(p-1) \cdot (q-1)}$
- if factorization of n into $p \cdot q$ is known, this is easy to do
- security of RSA is no better than the difficulty of factoring n into p, q

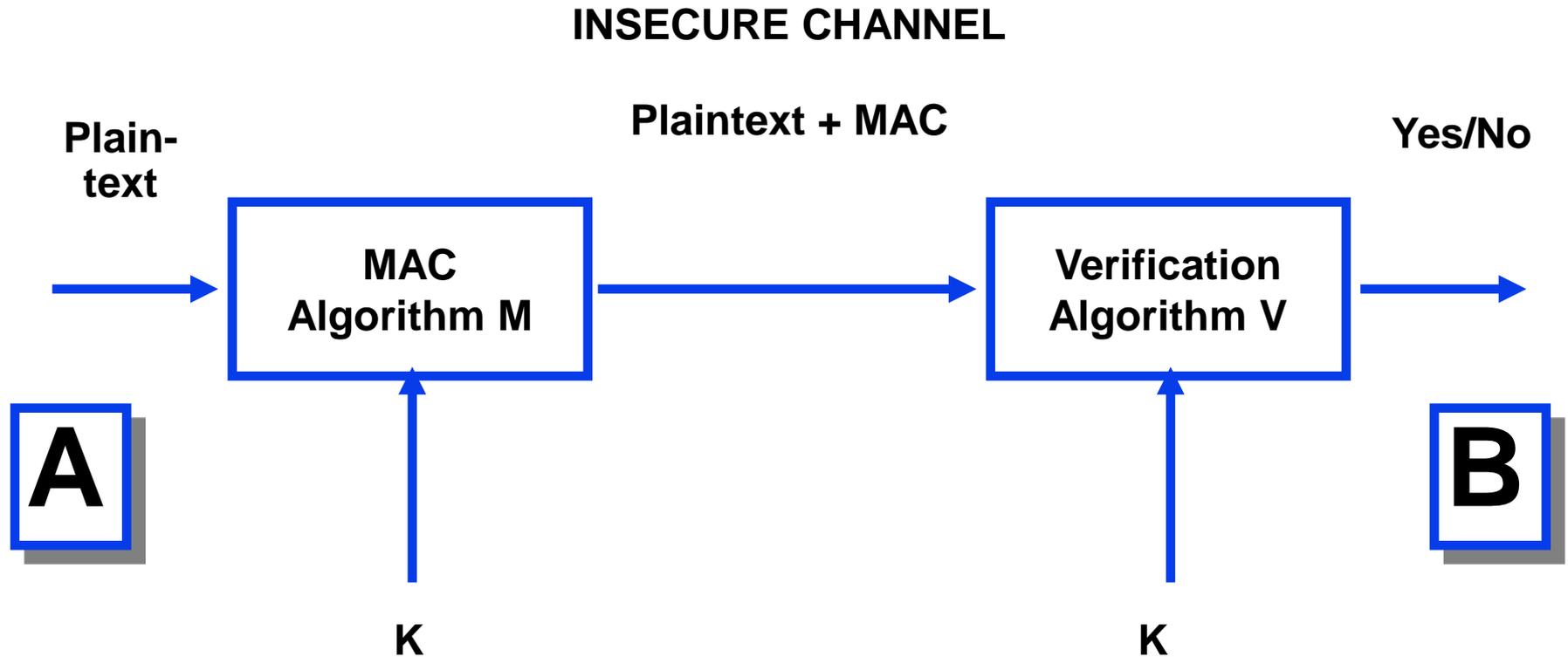
Asymmetric Digital Signatures

INSECURE CHANNEL



INSECURE CHANNEL



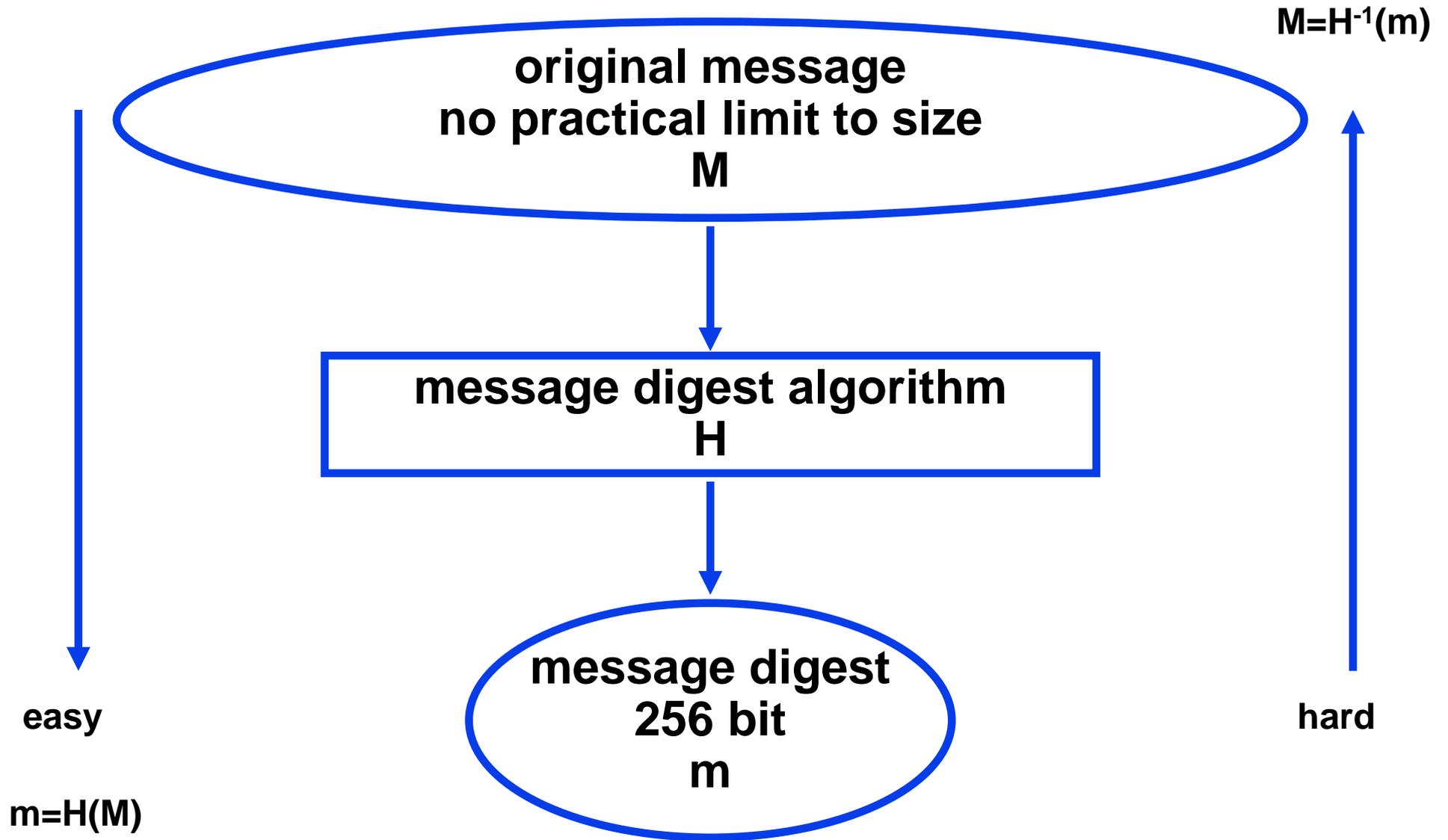


- RSA has a unique property, not shared by other public key systems
- Encryption and decryption commute
- $(M^e \bmod n)^d \bmod n = M$ encryption
- $(M^d \bmod n)^e \bmod n = M$ signature
- Same public key can be use for encryption and signature
 - ❖ But not recommended

Message Digest

- public key runs 1000 times slower than secret key
 - ❖ think 2g versus 4g on smartphone
- This large difference in speed is likely to remain
 - ❖ Maybe reduce to 100 times
- Use public keys to distribute secret keys, use secret keys to protect data

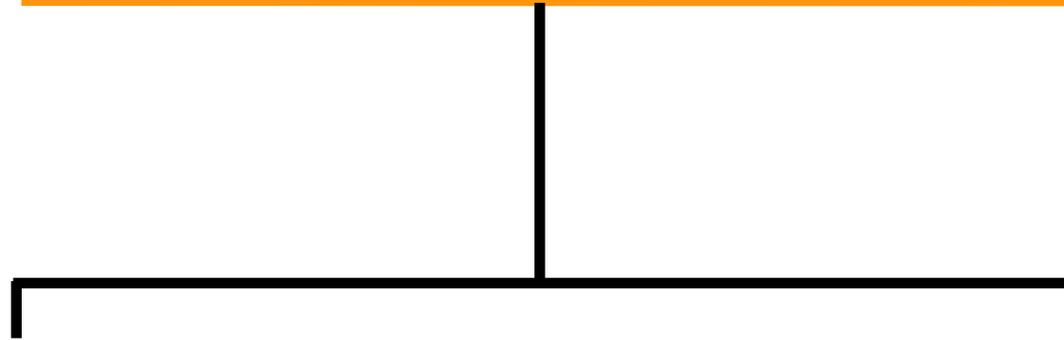
- public key runs 1000 times slower than secret key
 - ❖ think 2g versus 4g on smartphone
- This large difference in speed is likely to remain
 - ❖ Maybe reduce to 100 times
- Sign the message digest (or hash) not the message



- weak hash function
 - ❖ difficult to find M' such that $H(M')=H(M)$
- given M , $m=H(M)$ try messages at random to find M' with $H(M')=m$
 - ❖ 2^k trials on average, $k=128$ to be safe

- strong hash function
 - ❖ difficult to find any two M and M' such that $H(M')=H(M)$
- try pairs of messages at random to find M and M' such that $H(M')=H(M)$
 - ❖ $2^{k/2}$ trials on average, $k=256$ to be safe

Birthday paradox



Symmetric Encryption Based

CBC-MAC

MAC has same size as block size of underlying cryptosystem

CCM mode

Provides confidentiality and integrity

Message-Digest Based

HMAC

Hash the message and a secret key

MAC has same size as underlying hash function or can truncate

Revisiting after discussing message digests

Asymmetric Key Exchange



$y_A = a^{x_A} \text{ mod } p$
public key

private key

x_A

$y_B = a^{x_B} \text{ mod } p$
public key



private key

x_B

$$k = y_B^{x_A} \text{ mod } p = y_A^{x_B} \text{ mod } p = a^{x_A \cdot x_B} \text{ mod } p$$

system constants: p : prime number, a : integer

- security depends on difficulty of computing x given $y = a^x \pmod{p}$
- called the discrete logarithm problem

A

C

B

**Public keys need to be
authenticated**

Public-Key Certificates

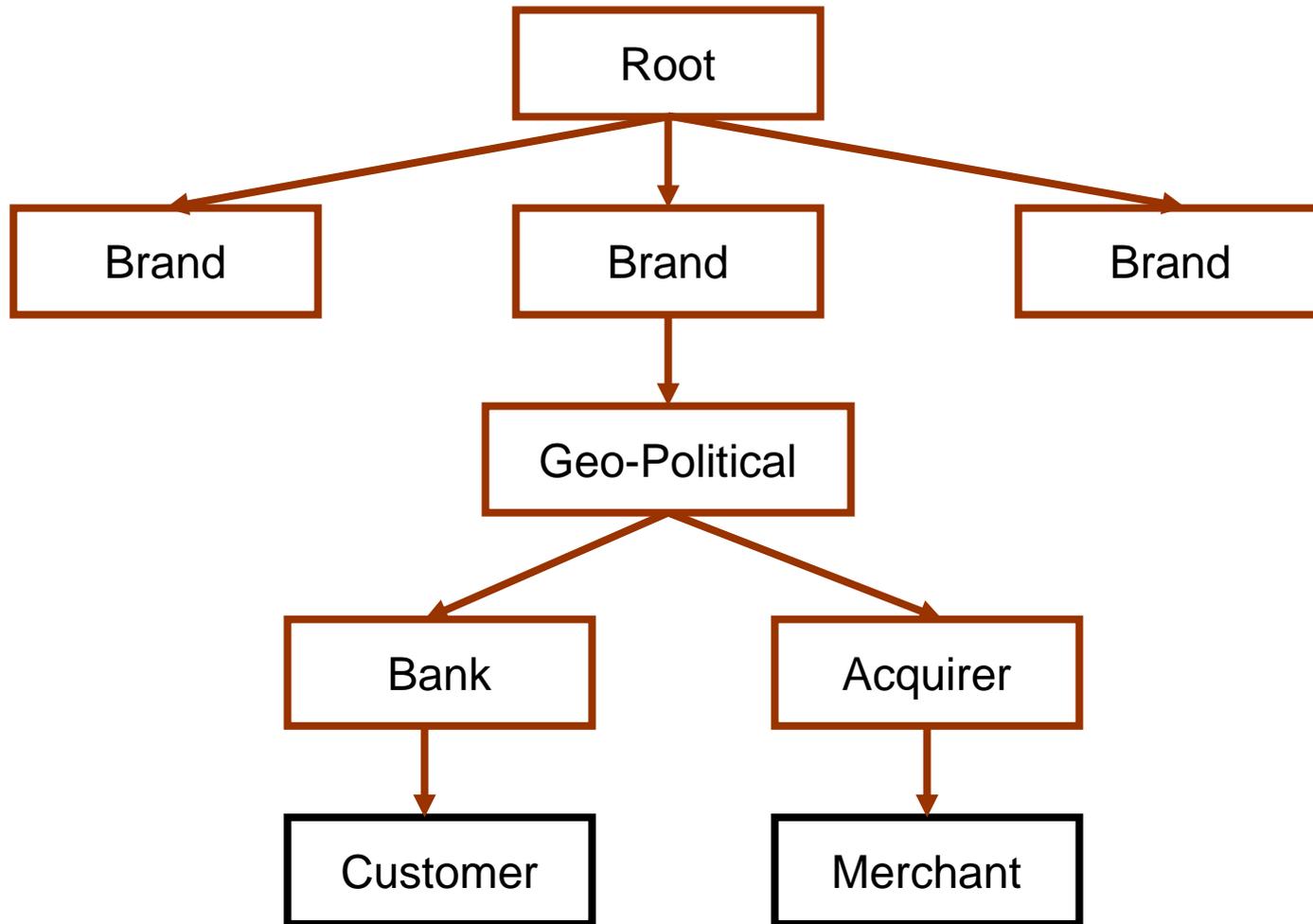
- authenticated distribution of public-keys
- public-key encryption
 - ❖ sender needs public key of receiver
- public-key digital signatures
 - ❖ receiver needs public key of sender
- public-key key agreement
 - ❖ both need each other's public keys

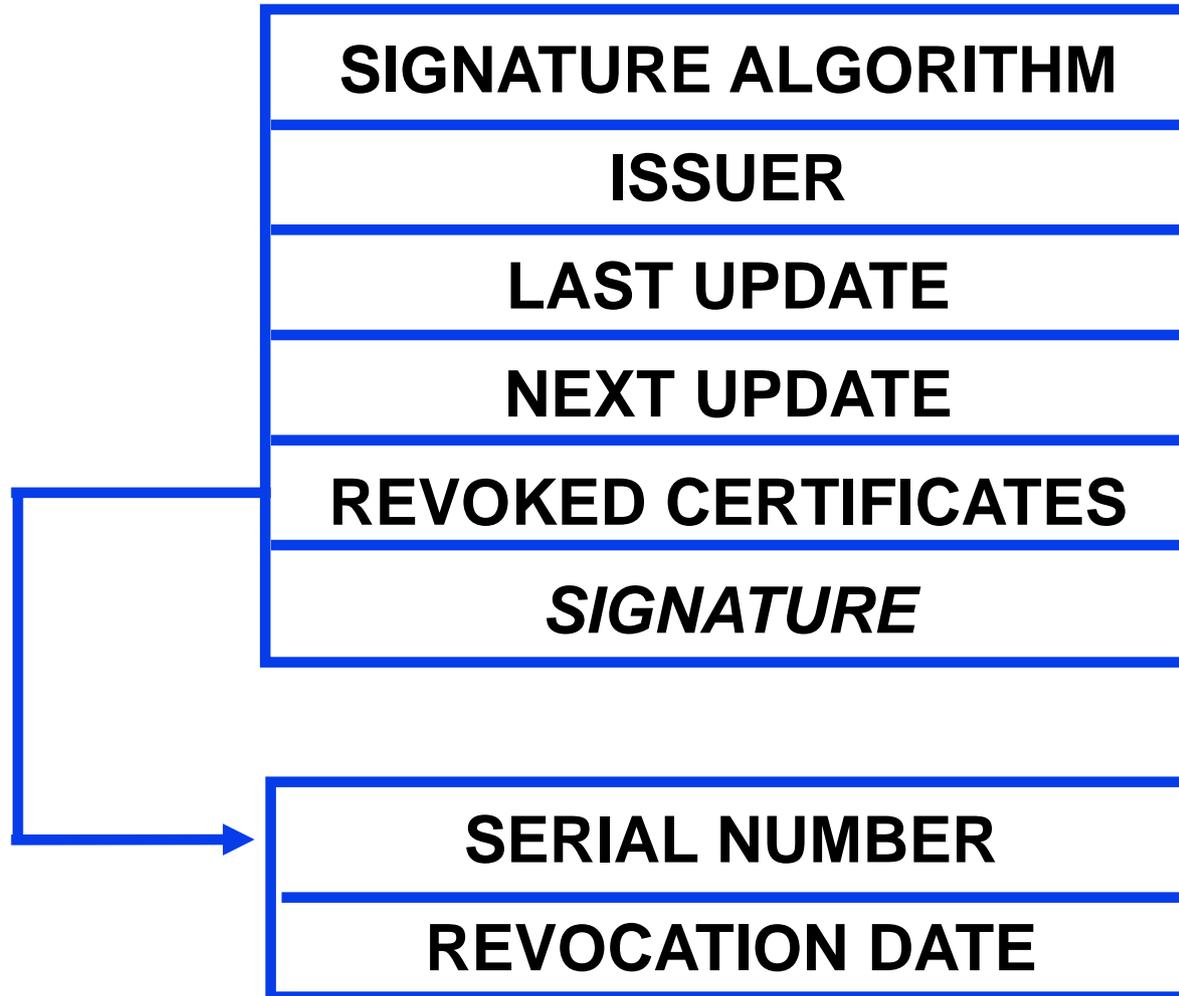
VERSION
SERIAL NUMBER
SIGNATURE ALGORITHM
ISSUER (Certificate Authority)
VALIDITY
SUBJECT
SUBJECT PUBLIC KEY INFO
<i>SIGNATURE</i>

1
1234567891011121314
RSA+SHA-3, 2048
C=US, S=TX, O=UTSA, OU=CS
1/1/17-12/31/18
C=US, S=TX, O=UTSA, OU=CS, CN=Ravi Sandhu
RSA, 2048, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
SIGNATURE

- how to acquire public key of the issuer to verify signature
- whether or not to trust certificates signed by the issuer for this subject
 - ❖ prefix rule is not universally applicable

1
1234567891011121314
RSA+SHA-3, 2048
C=US, S=VA, O=GMU, OU=ISE
1/1/17-12/31/18
C=US, S=TX, O=UTSA, OU=CS, CN=Ravi Sandhu
RSA, 2048, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
SIGNATURE

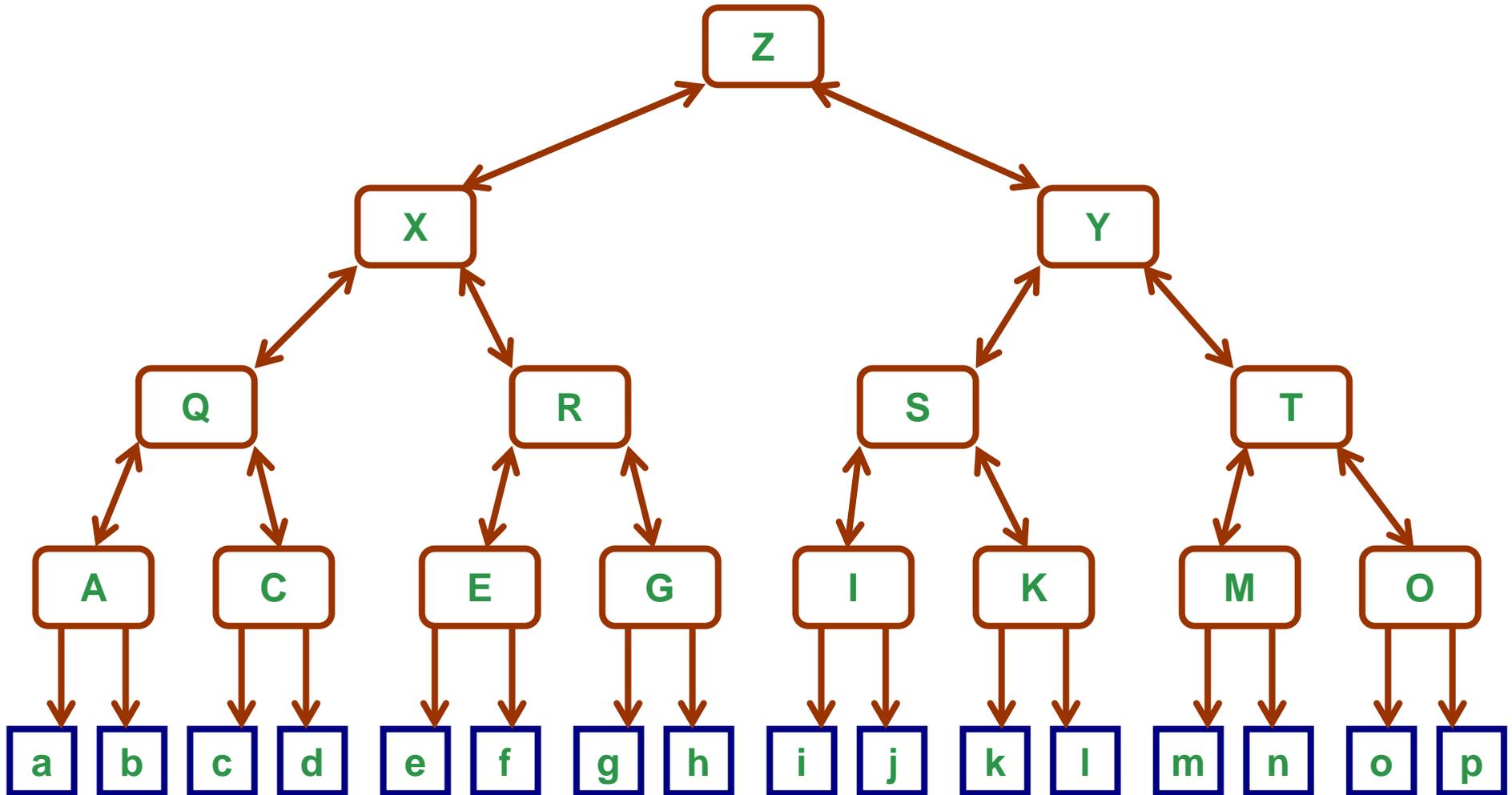


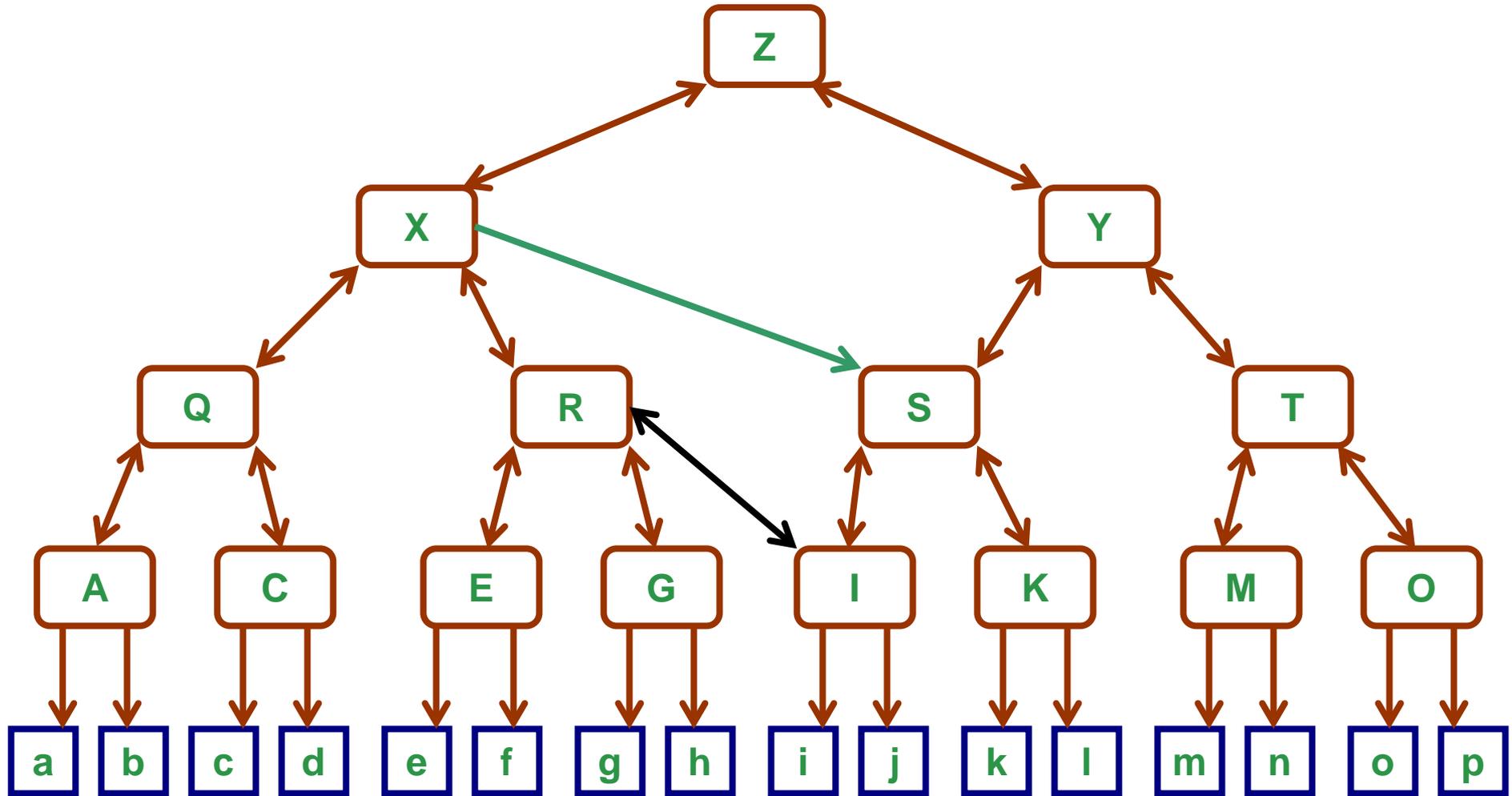


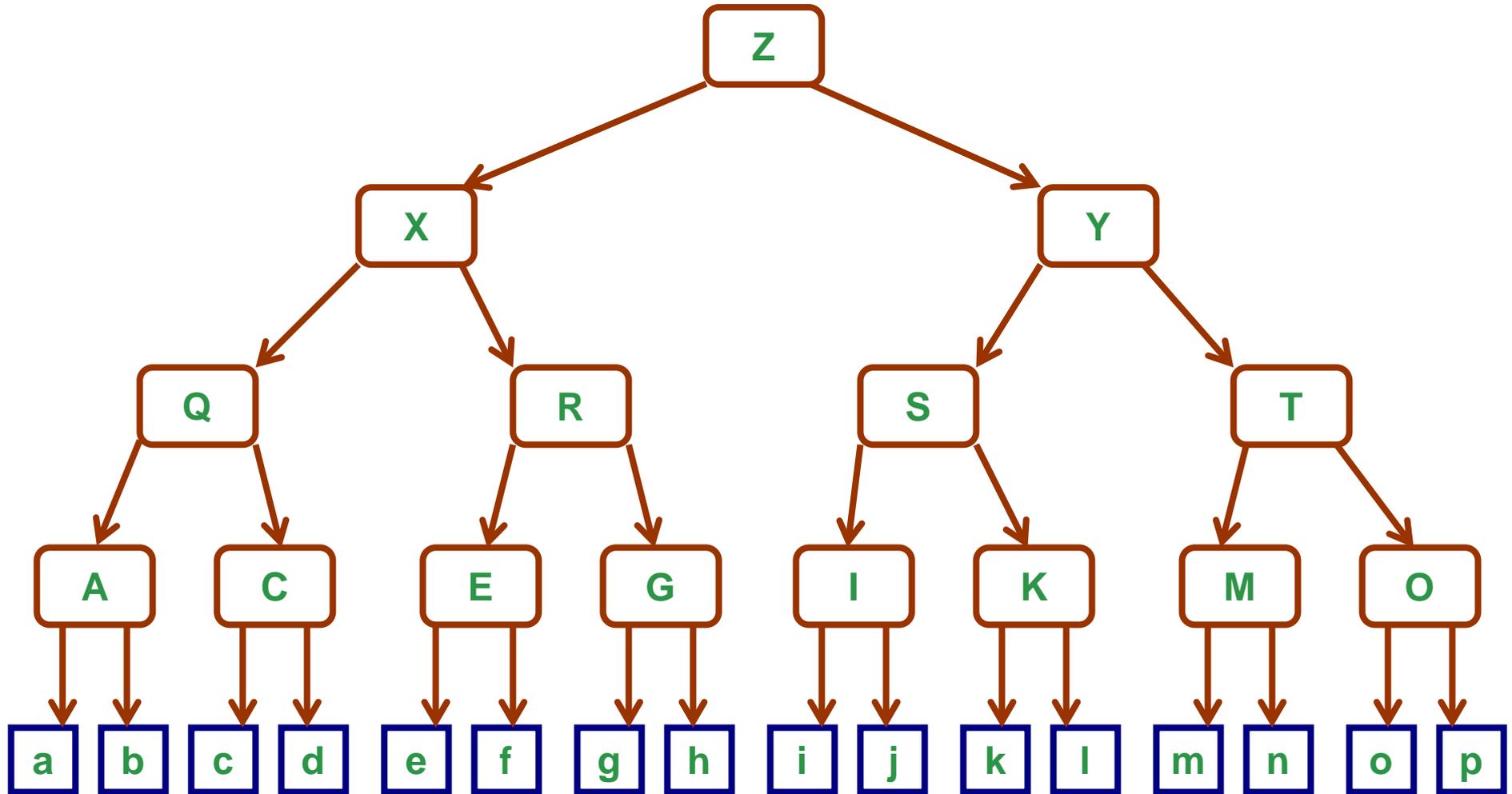
- X.509v1
 - ❖ very basic
- X.509v2
 - ❖ adds unique identifiers to prevent against reuse of X.500 names
- X.509v3
 - ❖ adds many extensions
 - ❖ can be further extended

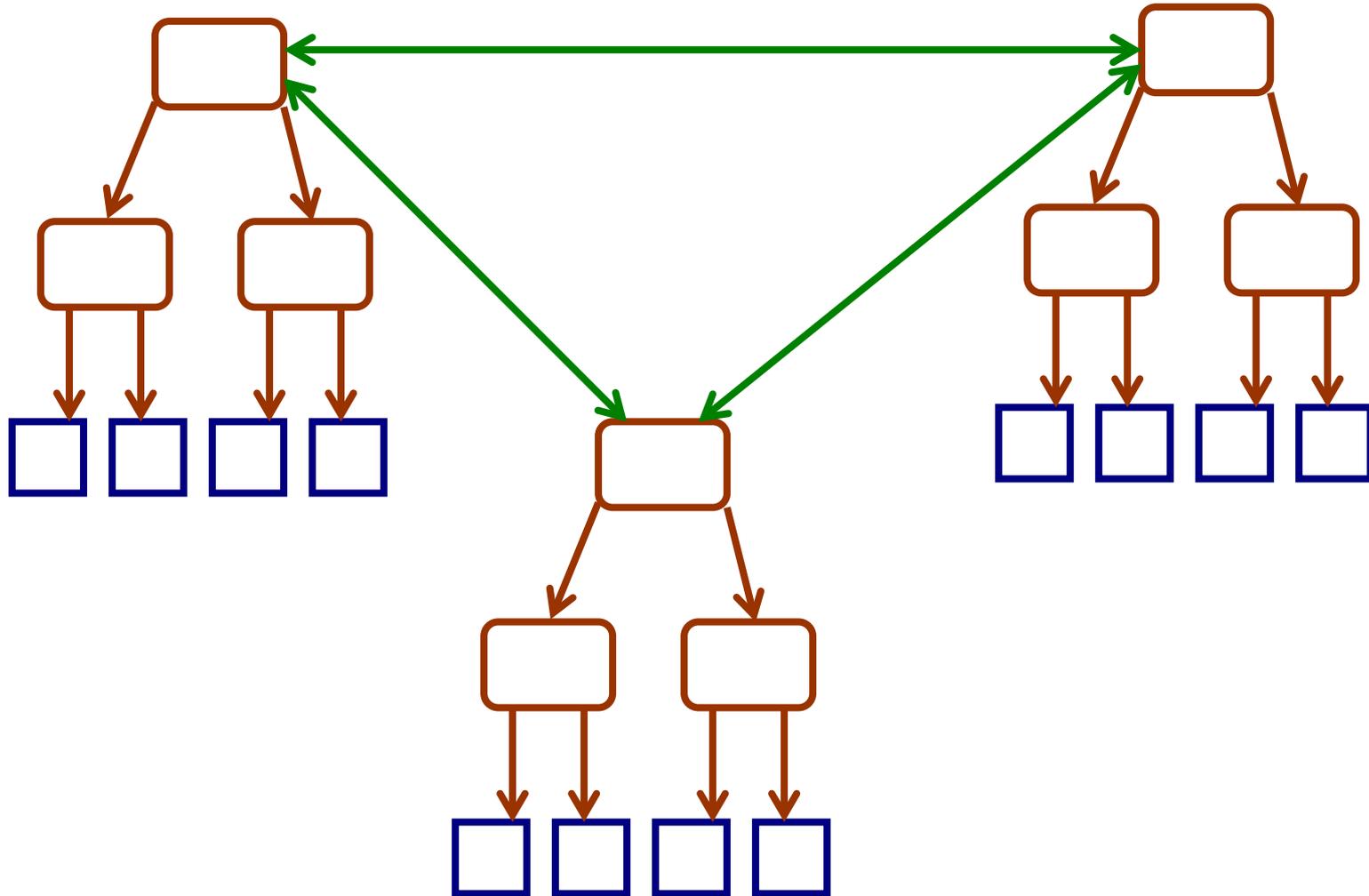
- distinguish various certificates
 - ❖ signature, encryption, key-agreement
- identification info in addition to X.500 name
 - ❖ internet names: email addresses, host names, URLs
- issuer can state policy and usage
 - ❖ ok for casual email but not for signing checks
- extensible
 - ❖ proprietary extensions can be defined and registered
- attribute certificates
 - ❖ to enable attribute-based authorization

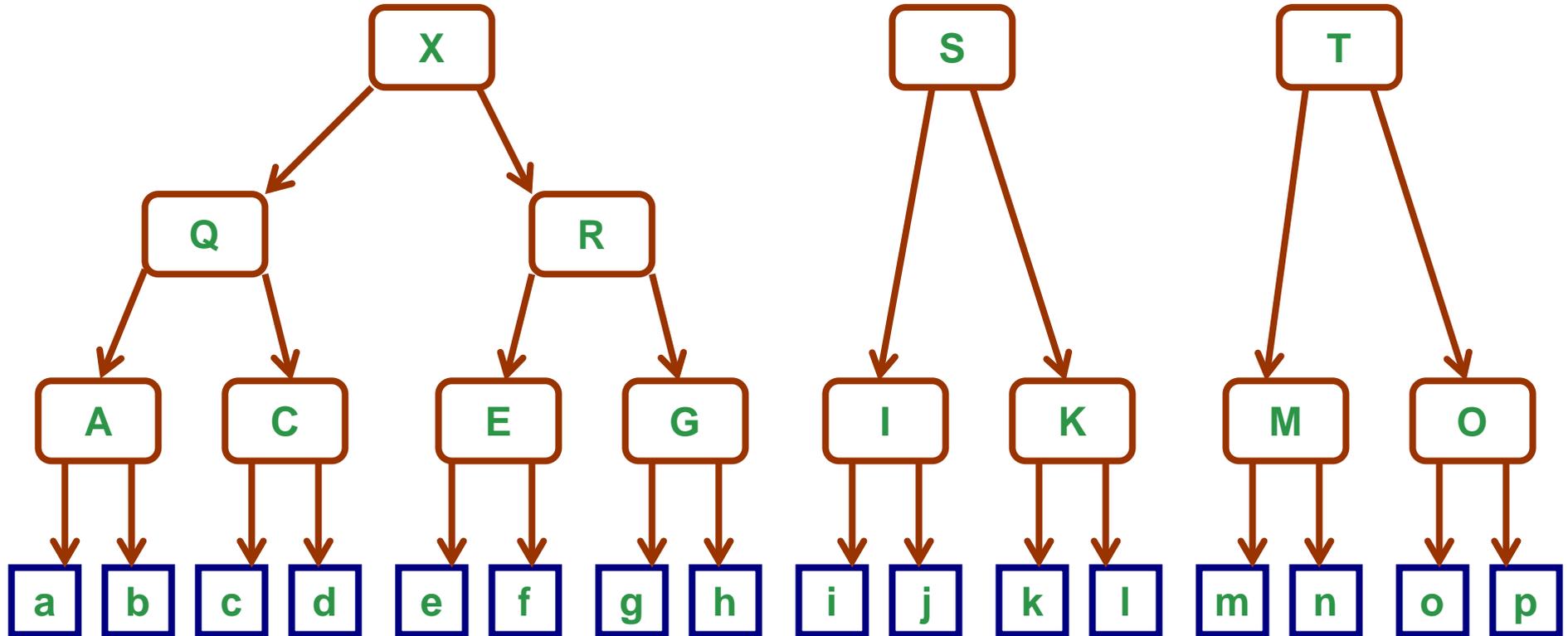
- CRL distribution points
- indirect CRLs
- delta CRLs
- revocation reason
- push CRLs



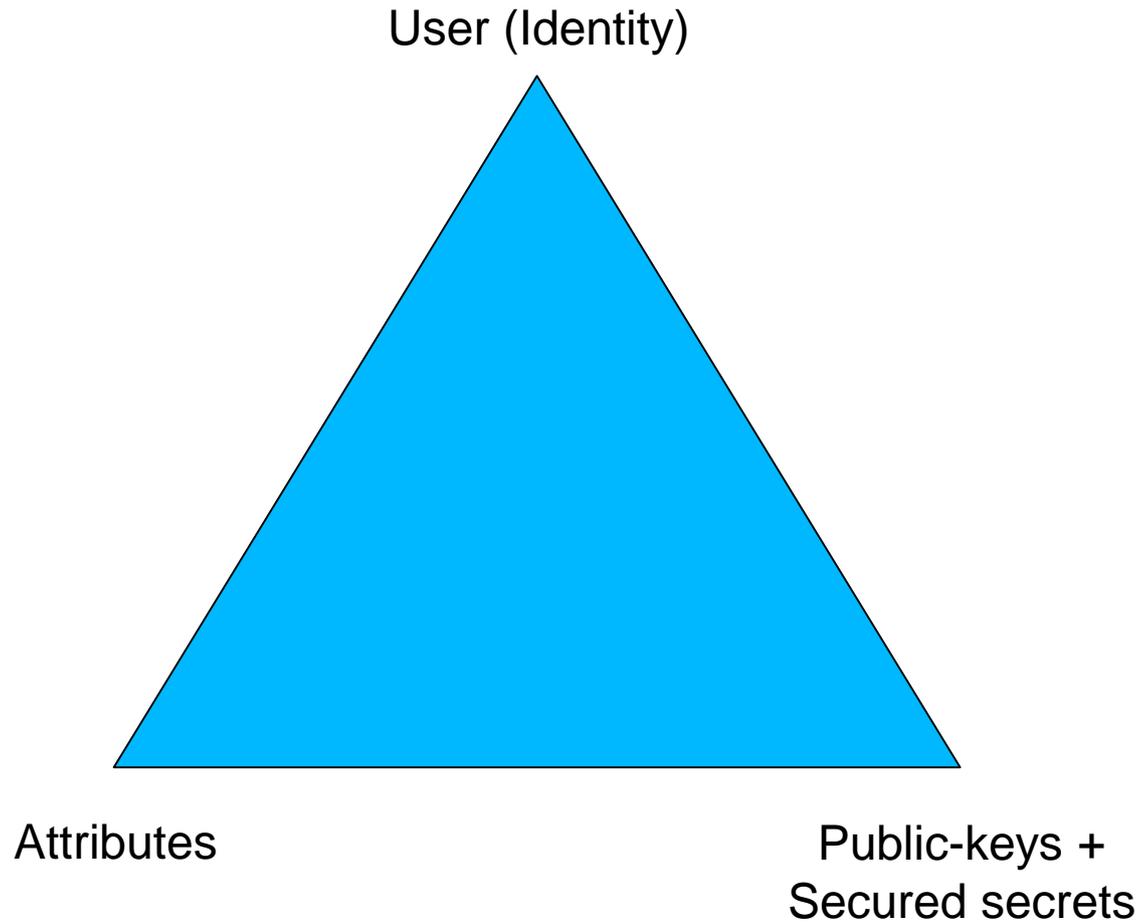








Model on the web today



Revisit from L5 on ABAC