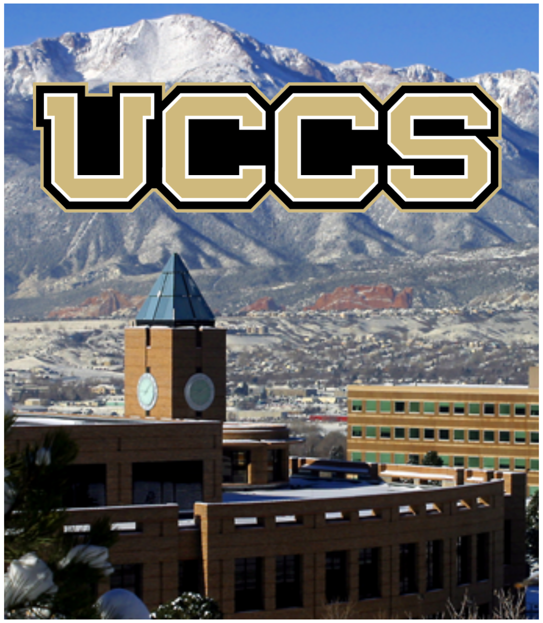


Cryptographic Hash and Integrity Protection

Digital Signature

Sang-Yoon Chang, Ph.D.

Module: Digital Signature

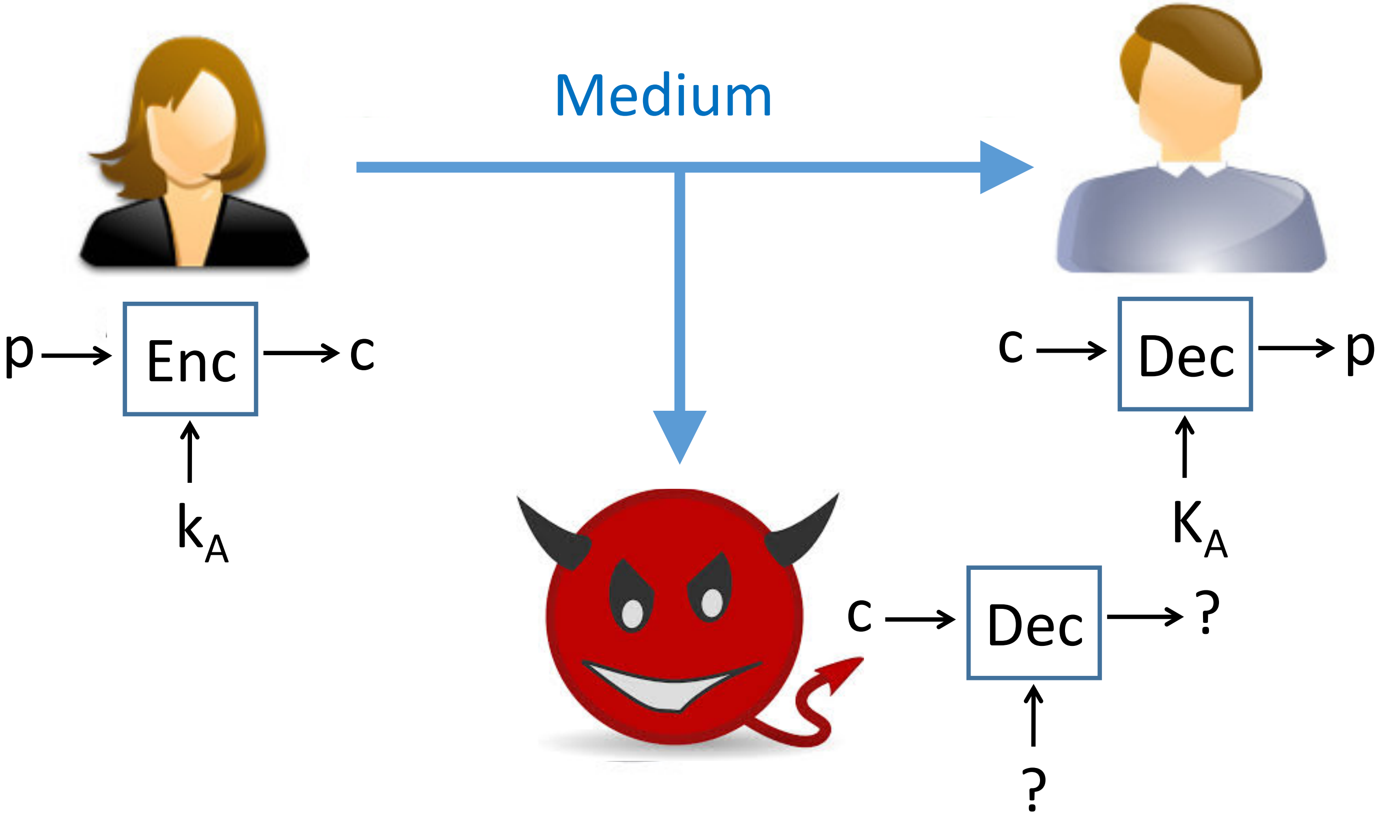
Asymmetric Cryptography and Integrity

Digital Signature Objectives

Digital Signature Requirements

Digital Signature Construction,
e.g., RSA and DSS

Asymmetric: Alice uses Alice’s private key k_A



Medium

p → Enc → c

k_A

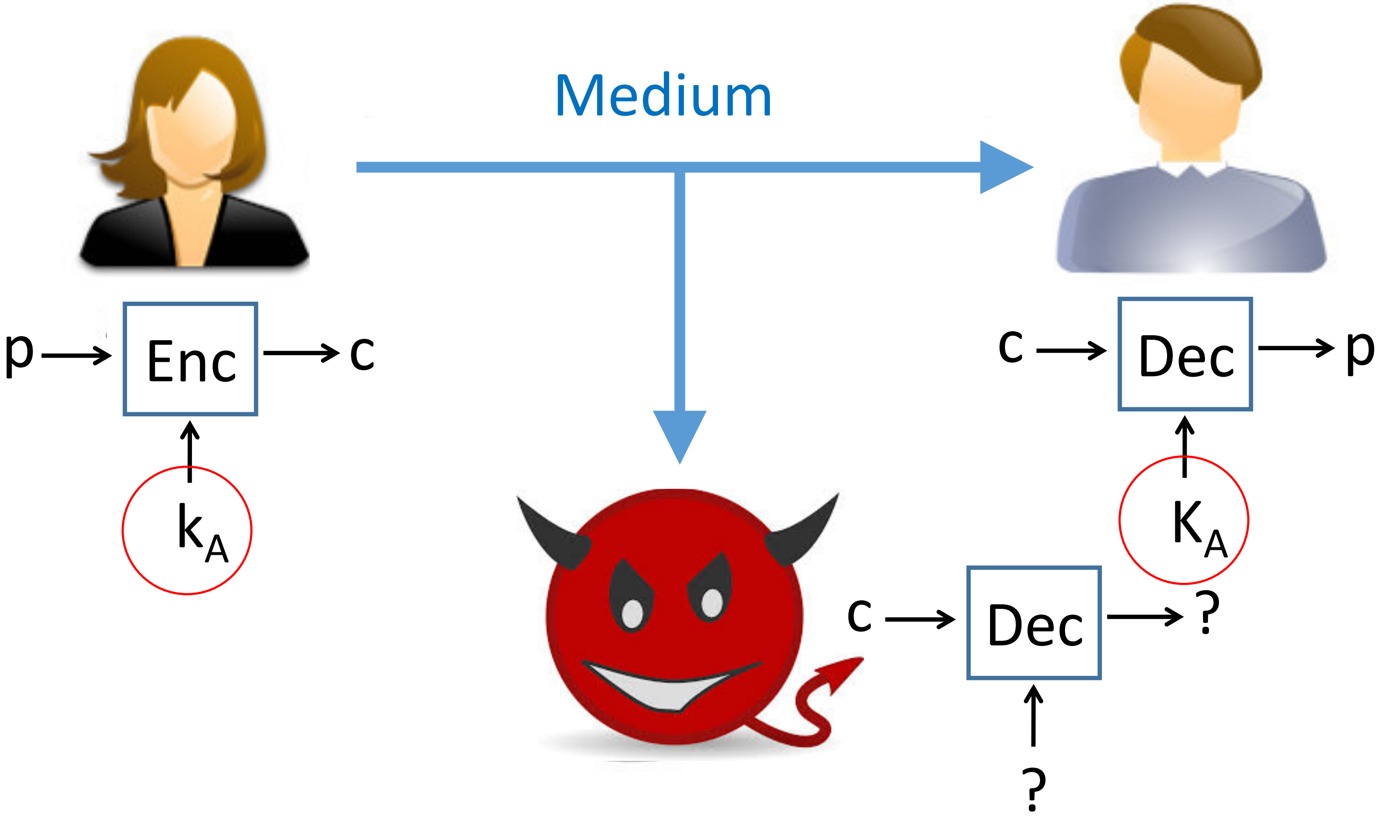
c → Dec → p

K_A

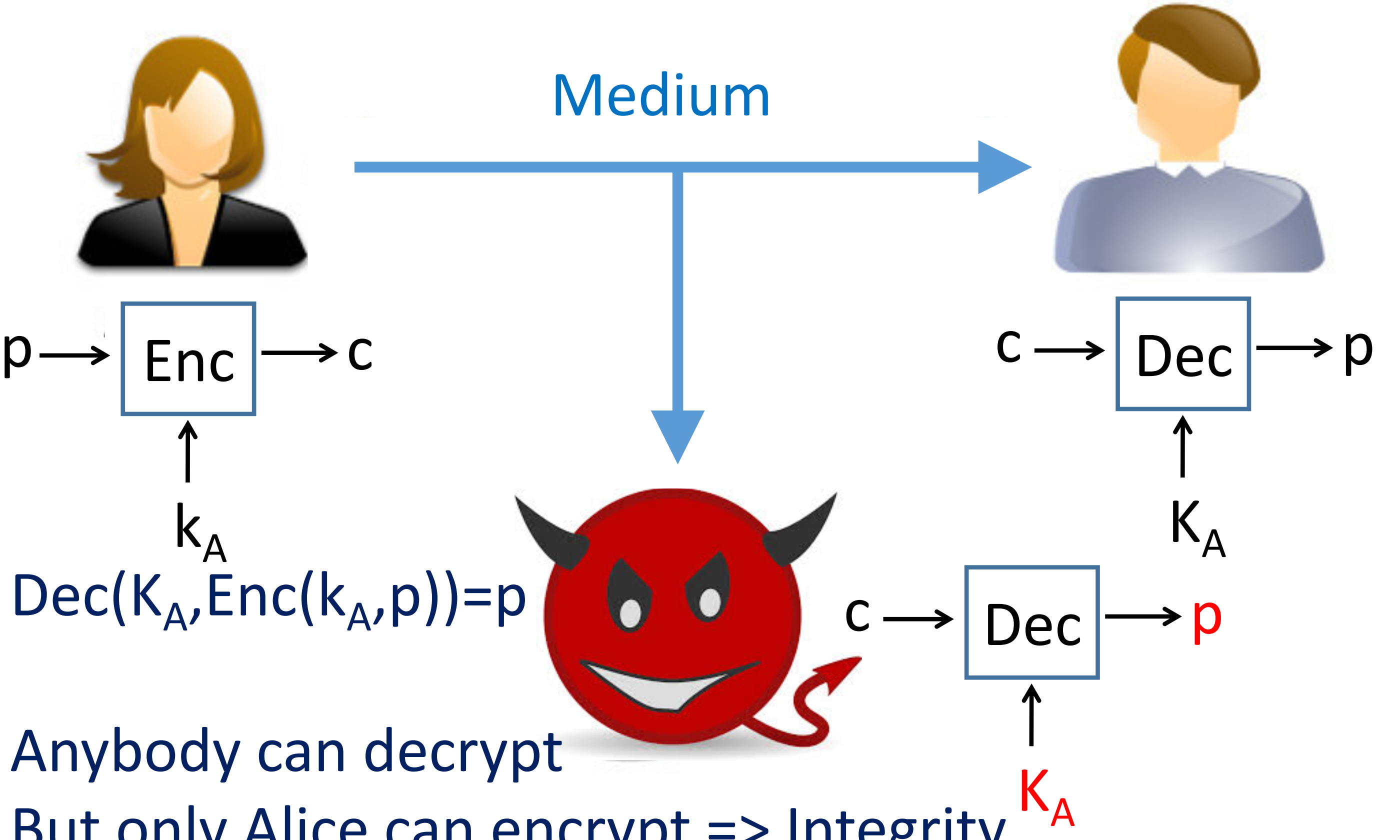
c → Dec → ?

?

Asymmetric: Alice uses Alice's private key k_A



Asymmetric: Alice uses Alice's private key k_A

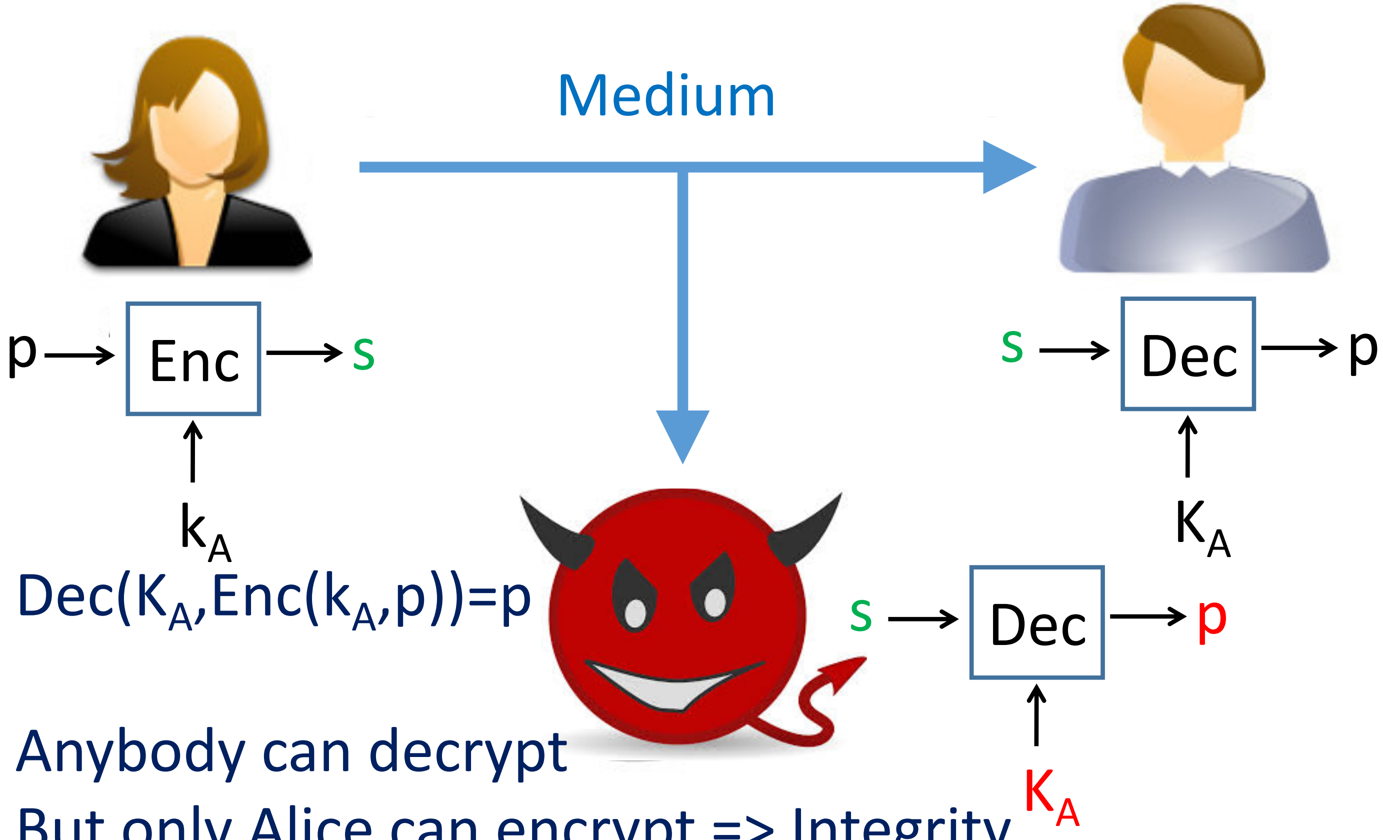


$Dec(K_A,Enc(k_A,p))=p$

Anybody can decrypt

But only Alice can encrypt => Integrity

Asymmetric: Alice uses Alice's private key k_A



Medium

$p \rightarrow$ Enc $\rightarrow s$

k_A

$s \rightarrow$ Dec $\rightarrow p$

K_A

$s \rightarrow$ Dec $\rightarrow p$

K_A

$Dec(K_A,Enc(k_A,p))=p$

Anybody can decrypt

But only Alice can encrypt => Integrity

Message Authentication Recap

Message authentication is to:

- Protect message integrity
- Sender authentication

Prevent threats, including:

- Masquerading/spoofing
- Content modification
- Sequence modification
- Timing modification

Message Authentication Recap

Message authentication is to:

- Protect message integrity
- Sender authentication

Prevent threats, including:

- Masquerading/spoofing
- Content modification
- Sequence modification
- Timing modification

It does not address trust between parities

Digital Signature

Prevent threats:

- Another user spoofs the sender
- Receiver forges a received message
- Sender deny sending message

Digital Signature

Prevent threats:

- Another user spoofs the sender
- Receiver forges a received message
- Sender deny sending message

Needs to be:

- Verify author and the time of signature
- Authenticate content at time of signature
- Verifiable by other, e.g., resolve disputes

Digital Signature

Prevent threats:

- Another user spoofs the sender
- Receiver forges a received message
- Sender deny sending message

Needs to be:

- Verify author and the time of signature
- Authenticate content at time of signature
- Verifiable by others, e.g., resolve disputes

Digital Signature Requirements

Depends on the message being signed

Use information unique to the sender

Digital Signature Requirements

Depends on the message being signed

Use information unique to the sender

Easy to produce

Easy to recognize and verify

Digital Signature Requirements

Depends on the message being signed

Use information unique to the sender

Easy to produce

Easy to recognize and verify

Infeasible to forge

Digital Signature Requirements

Depends on the message being signed

Use information unique to the sender

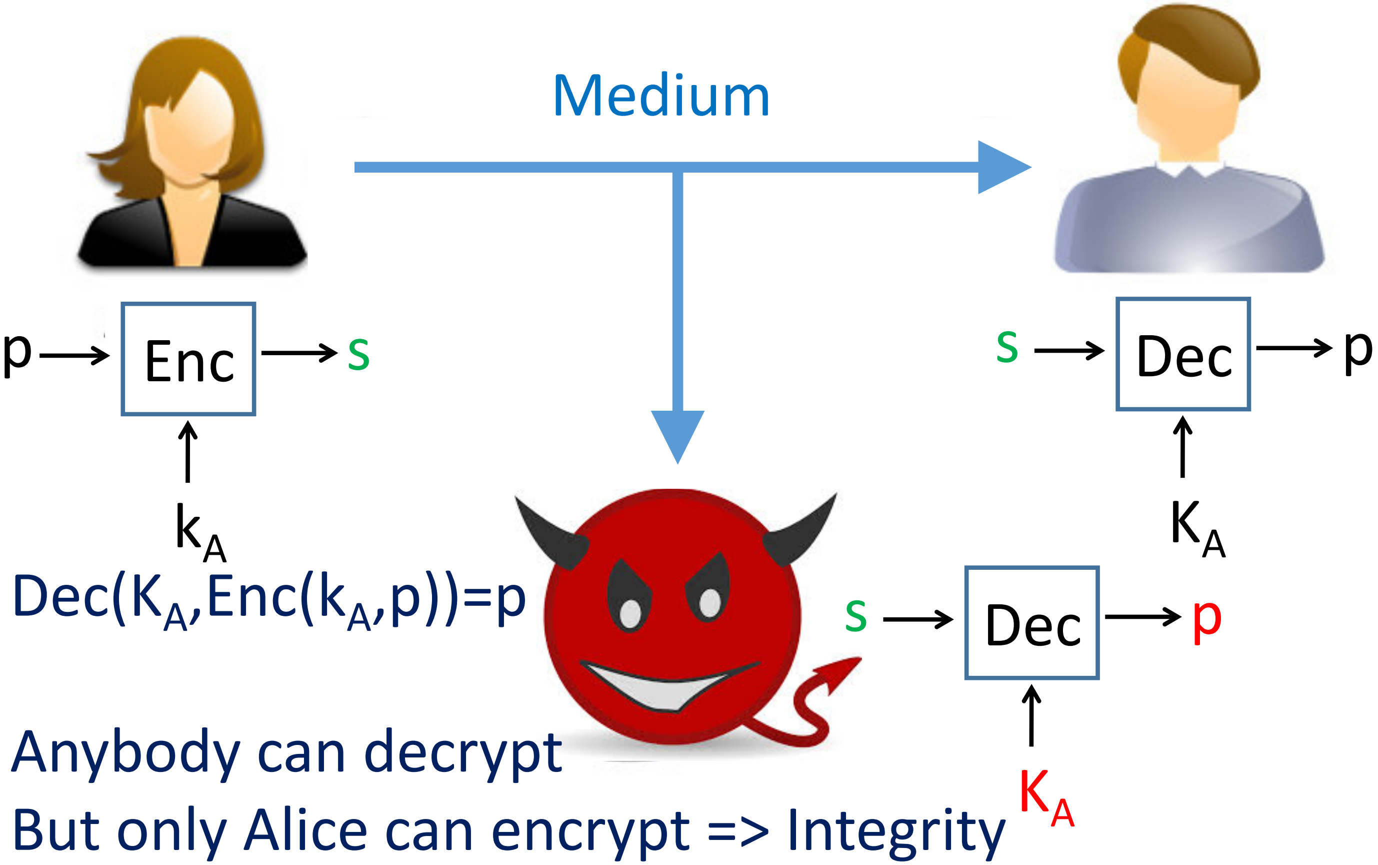
Easy to produce

Easy to recognize and verify

Infeasible to forge

Able to retain a copy in storage

Asymmetric: Alice uses Alice's private key k_A



Medium

p → Enc → s

k_A

s → Dec → p

K_A

s → Dec → p

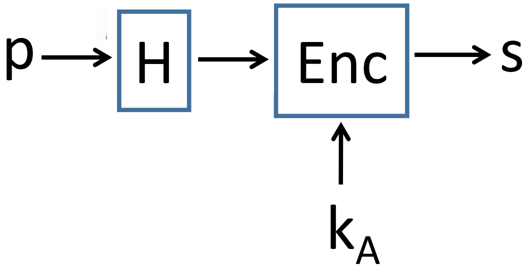
K_A

$Dec(K_A,Enc(k_A,p))=p$

Anybody can decrypt

But only Alice can encrypt => Integrity

Digital Signature



p

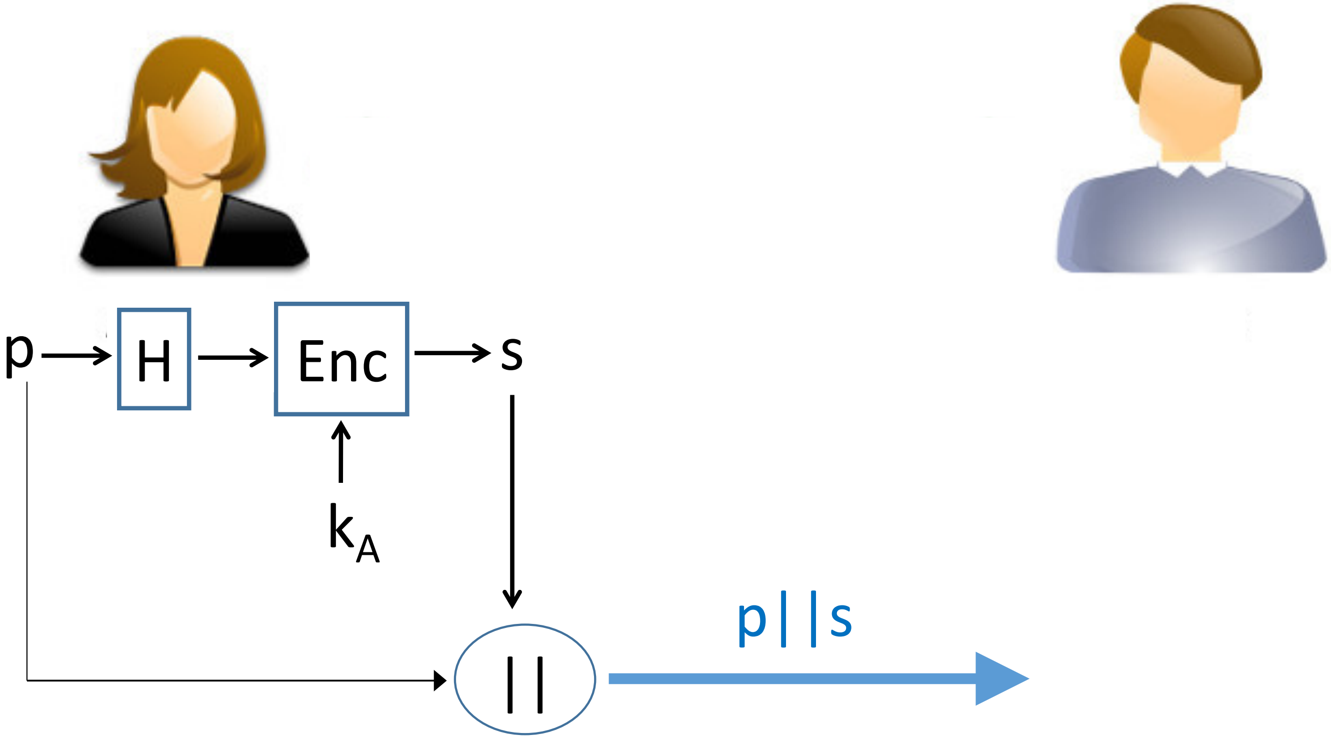
H

Enc

s

k_A

Digital Signature



p

H

Enc

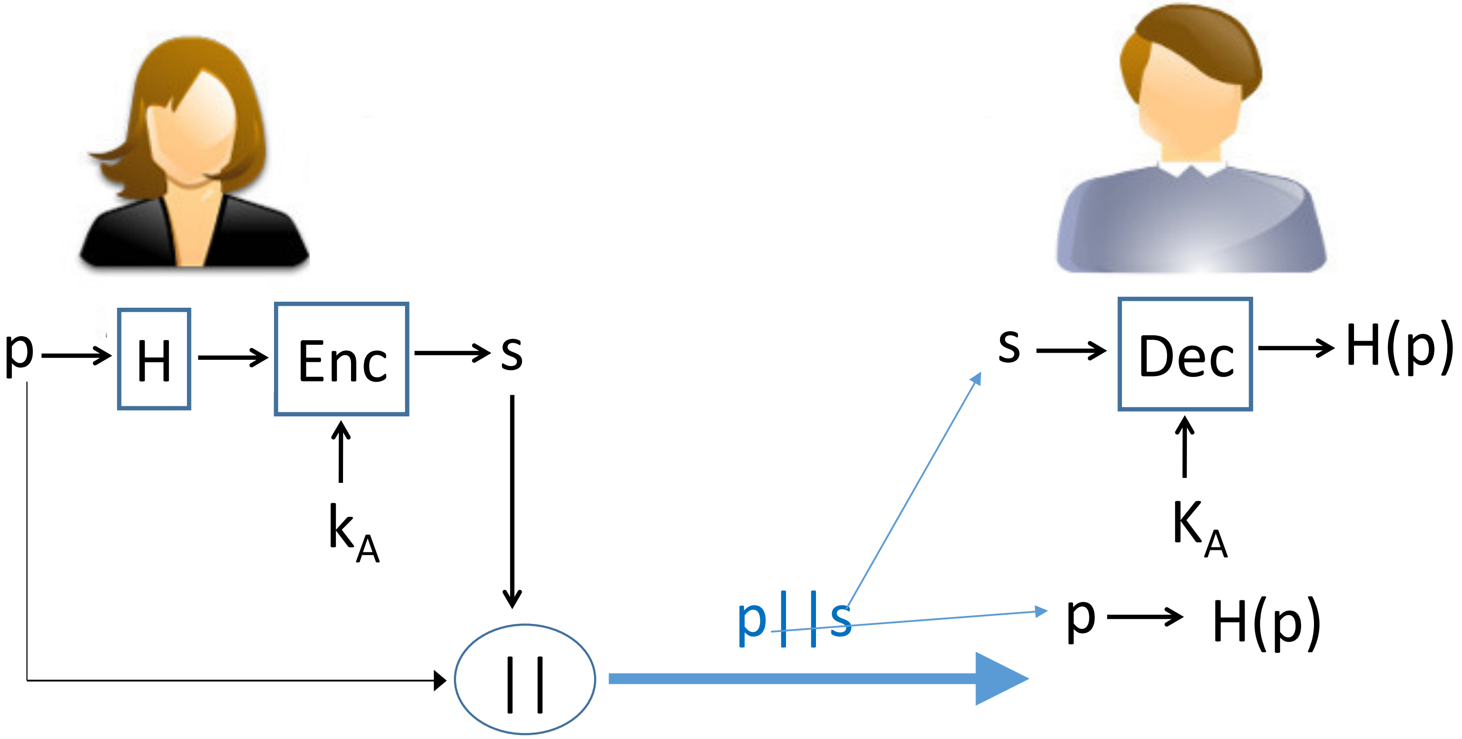
s

k_A

$||$

$p||s$

Asymmetric: Alice uses Alice's private key k_A



p → H → Enc → s

k_A

||

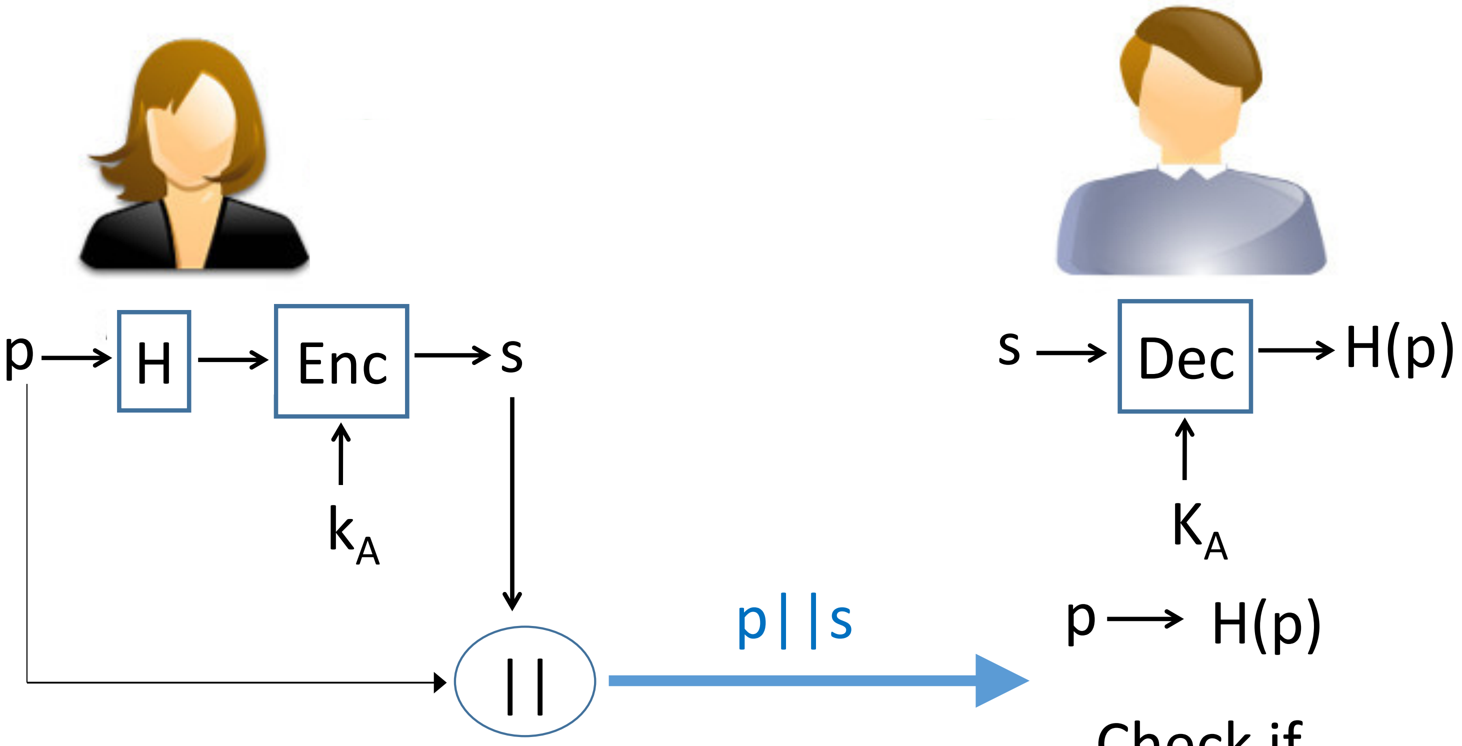
p||s

s → Dec → H(p)

K_A

p → H(p)

Asymmetric: Alice uses Alice's private key k_A



p → H → Enc → s

k_A

p || s

s → Dec → H(p)

K_A

p → H(p)

Check if
match?