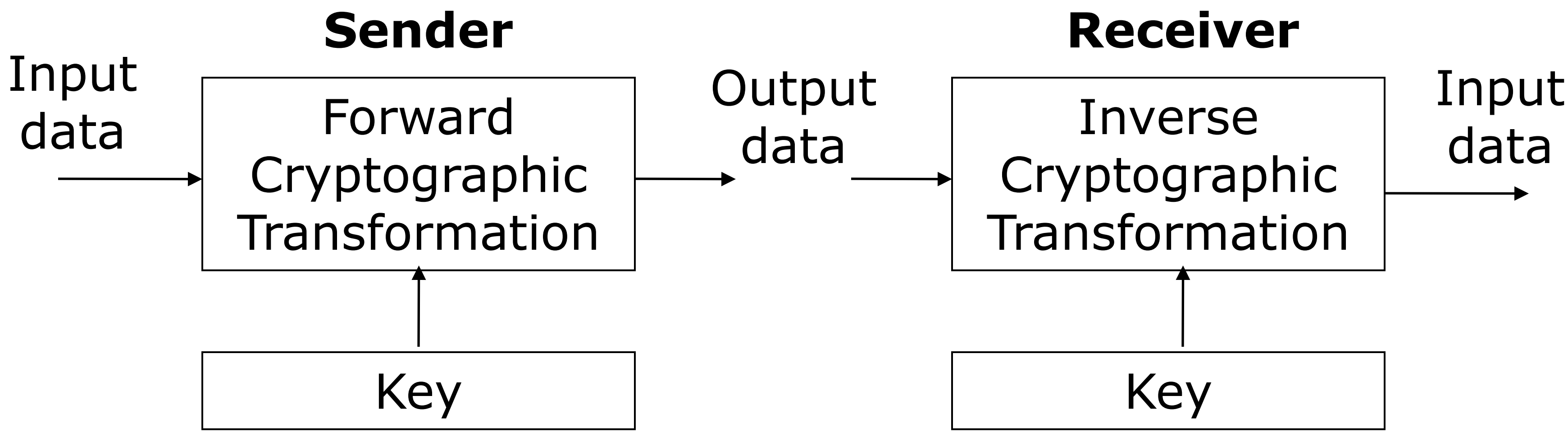
Digital Signature Schemes

Introduction

- *Cryptography* – art & science of preventing users from unauthorized or illegal actions towards information, networking resources and services.
- *Cryptographic transformation* – conversion of input data into output data using a *cryptographic key*.
- *Cryptosystem* – *forward* and *inverse* cryptographic transformation pair

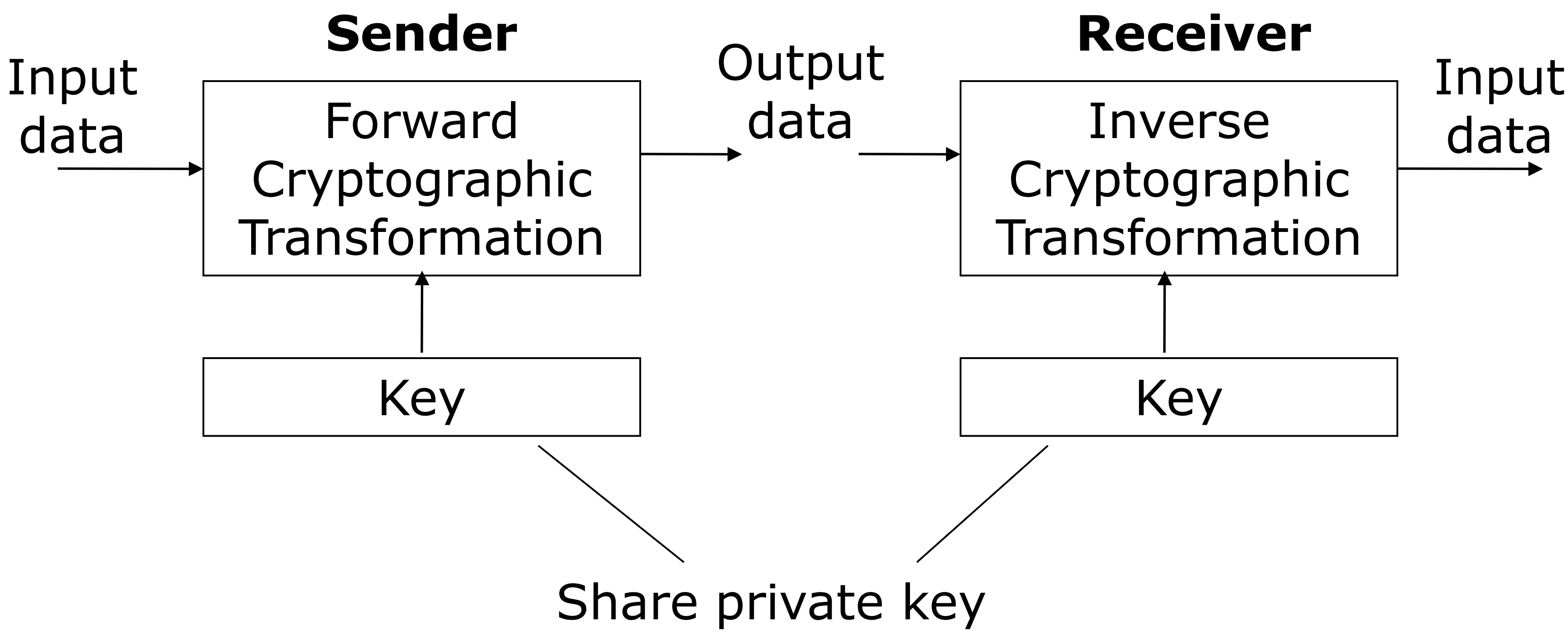
A Cryptosystem



Types of Cryptosystems

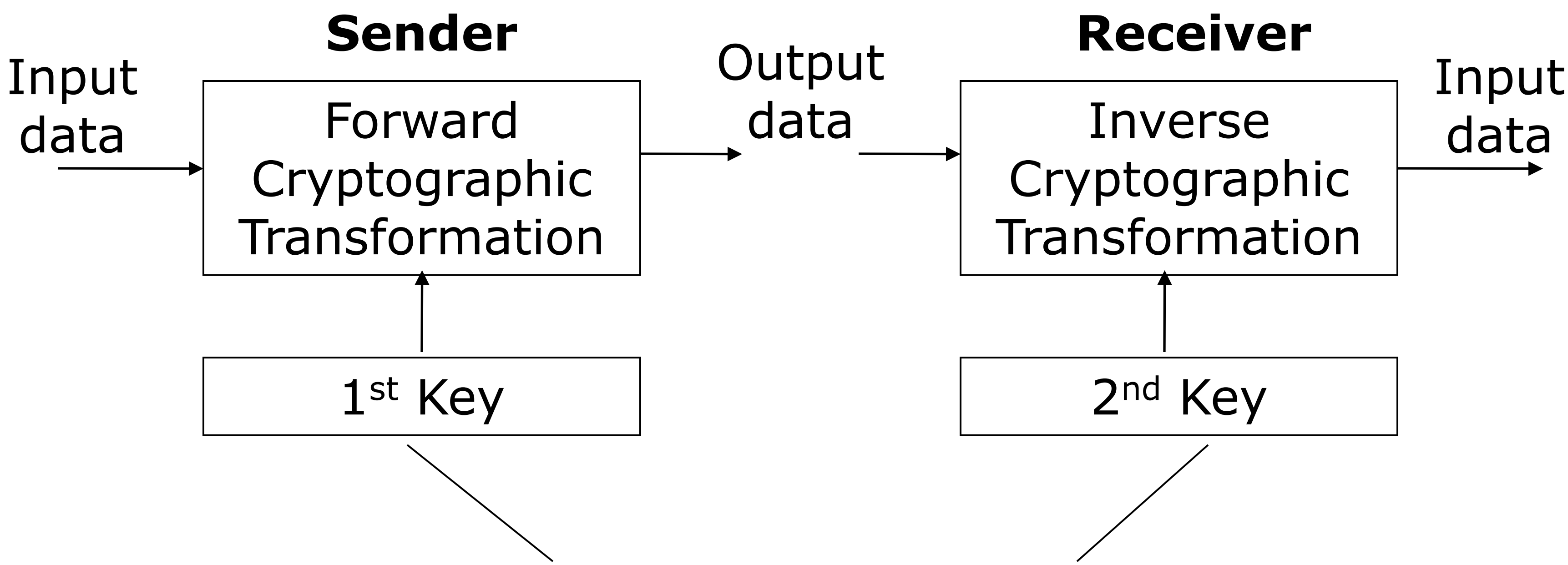
- *Private key* cryptosystem – a private key is shared between the two communicating parties which must be kept secret between themselves.
- *Public key* cryptosystem – the sender and receiver do not share the same key and one key can be public and the other can be private

Types of Cryptosystems



A Private Key Cryptosystem

Types of Cryptosystems



Do not share the same key information and one key may be public

A Public Key Cryptosystem

Digital Signatures

- *Encryption*, *message authentication* and *digital signatures* are all tools of modern cryptography.
- A signature is a technique for non-repudiation based on the public key cryptography.
- The creator of a message can attach a code, the signature, which guarantees the source and integrity of the message.

Properties of Signatures

- Similar to handwritten signatures, digital signatures must fulfill the following:
  - ✓ Must not be forgeable
  - ✓ Recipients must be able to verify them
  - ✓ Signers must not be able to repudiate them later
- In addition, digital signatures cannot be constant and must be a function of the entire document it signs

Types of Signatures

- *Direct digital signature* – involves only the communicating parties
  - ✓ Assumed that receiver knows public key of sender.
  - ✓ Signature may be formed by (1) encrypting entire message with sender's private key or (2) encrypting hash code of message with sender's private key.
  - ✓ Further encryption of entire message + signature with receiver's public key or shared private key ensures confidentiality.

Types of Signatures

- Problems with direct signatures:
  - ✓ Validity of scheme depends on the security of the sender's private key $\Rightarrow$ sender may later deny sending a certain message.
  - ✓ Private key may actually be stolen from X at time T, so timestamp may not help.

Types of Signatures

- *Arbitrated digital signature* – involves a trusted third party or arbiter
  - ✓ Every signed message from sender, X, to receiver, Y, goes to an arbiter, A, first.
  - ✓ A subjects message + signature to number of tests to check origin & content
  - ✓ A dates the message and sends it to Y with indication that it has been verified to its satisfaction

Basic Mechanism of Signature Schemes

- A key generation algorithm to randomly select a public key pair.
- A signature algorithm that takes message + private key as input and generates a signature for the message as output
- A signature verification algorithm that takes signature + public key as input and generates information bit according to whether signature is consistent as output.

Digital Signature Standards

- NIST FIPS 186 Digital Signature Standard (DSS)

- El Gamal

- RSA Digital Signature
  - ISO 9796
  - ANSI X9.31
  - CCITT X.509

DSS

- Public-key technique.
- User applies the Secure Hash Algorithm (SHA) to the message to produce message digest.
- User's private key is applied to message digest using *DSA* to generate signature.

Global Public-Key Components	
p	A prime number of L bits where L is a multiple of 64 and $512 \leq L \leq 1024$
q	A 160-bit prime factor of p-1
g	$= h^{(p-1)/q} \bmod p$, where h is any integer with $1<h< p-1$, such that $(h^{(p-1)/q} \bmod p)>1$
User's Private Key	
x	A random or pseudorandom integer with $0<x<q$
User's Public Key	
y	$= g^{x} \bmod p$
User's Per-Message Secret Number	
k	A random or pseudorandom integer with $0<k<q$
Signing	
	$r = (g^{k} \bmod p) \bmod q$ $s = [k^{-1} (\mathrm{H}(\mathrm{M}) = xr)] \bmod q$ Signature = (r, s)
Verifying	
	$w = (s')^{-1} \bmod q$ $u_1 = [\mathrm{H}(\mathrm{M}')w] \bmod q$ $u_2 = (r')w \bmod q$ $v = [(g^{u1}y^{u2}) \bmod p] \bmod q$ Test: $v = r'$

The Digital Signature Algorithm (DSA)

DSS

- DSA
  - M = message to be signed
  - H(M) = hash of M using SHA
  - M', r', s' = received versions of M, r, s

El Gamal Signature Scheme

- A variant of the DSA.
- Based on the assumption that computing discrete logarithms over a finite field with a large prime is difficult.
- Assumes that it is computationally infeasible for anyone other than signer to find a message M and an integer pair (r, s) such that $a^M = y^r r^s (\text{mod } p)$.

El Gamal Signature Scheme

Parameters of El Gamal	
p	A large prime number such that p-1 has a large prime factor
x	The private key information of a user where $x<p$
a	A primitive element of the finite field for the prime p
y	$= a^x \bmod p$
(p,a,y)	The public key information

El Gamal Signature Scheme

Step 1	Randomly choose an integer k such that $(k, p\text{-}1) = 1$, $1<k<p\text{-}1$, and k has not been used to sign a previous message
Step 2	Calculate $r = a^k \pmod{p}$
Step 3	Find s such that $M = xr + ks \pmod{(p\text{-}1)}$
Step 4	Collect the pair (r, s) as the digital signature on the message M

Since, $M = xr + ks \pmod{(p\text{-}1)}$

$\Rightarrow a^M = a^{(xr+ks)} = a^{xr}a^{ks} = y^r r^s \pmod{p}$

$\Rightarrow$ Given M and (r, s), the receiver or 3rd party can verify the signature by checking whether $a^M = y^r r^s \pmod{p}$ holds or not.

RSA Digital Signature Scheme

- Based on the difficulty of factoring large numbers.
- Given *M*, RSA digital signature can be produced by encrypting either *M* itself or a digest of *M* using the private signature key *s*.
- Signature, $S = w^s \bmod n$, where *w* is message to be signed or message digest and $n = pq$ (*p* and *q* are large primes).
- Verification: $w = S^v \bmod n$, where (v, n) is the public verification key.

Conclusions

- Digital signatures are an effective mechanism used for authenticity and non-repudiation of messages.
- Several signature schemes exist, but DSS is probably the most popular.
- Digital signatures may be expanded to be used as digital pseudonyms which would prevent authorities from figuring out a sender's identity, for example by cross-matching

Thank you!