Information Transmission
Chapter 6, Public key cryptography

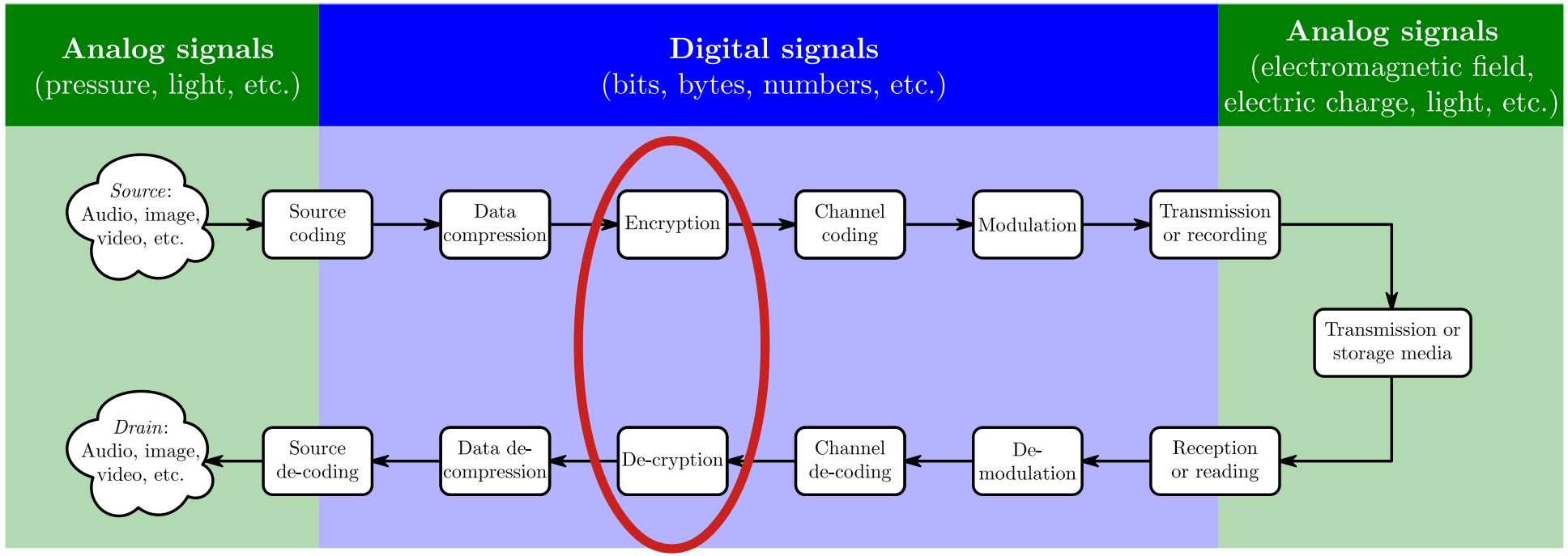
OVE EDFORS / SARA GUNNARSSON
ELECTRICAL AND INFORMATION TECHNOLOGY

Learning outcomes

- After this lecture the student should
  - understand the concept of one-way functions and specifically trapdoor one-way functions,
  - understand what a two-key public-key cryptosystem is and how trapdoor one-way functions can be used to create such a system,
  - understand Euler's totient function and how it can be used to create a trapdoor one-way function,
  - know how to use Euclid's algorithm to calculate the greatest common divisor (gcd) of two natural numbers and understand the relation to Bezout's identity,
  - be able to perform the basic operations of Rivest-Shamir-Adelman (RSA) encryption and decryption, and
  - understand how a digital signature is created using trapdoor one-way functions.

LUND UNIVERSITY

Where are we in the BIG PICTURE?



Public-key crypto

Lecture relates to pages 228-239 in textbook.

LUND UNIVERSITY

One-way functions

It is possible to exchange secret keys without using a secure channel!

Diffie and Hellman introduced the concepts of *one-way functions* and *trapdoor one-way functions*.

A remarkable idea that dramatically changed the cryptological research.

A one-way function is a function y=*f(x)* that is “easy” to compute for all *x*, but it is computationally infeasible to find *x* if you know only *y=f(x).*

Trapdoor one-way functions

- A trapdoor one-way function is a family of invertible functions f_K such that
  - when K is known, we can easily find algorithms E_K and D_K that compute $f_K(x)$ and its inverse $f_K^{-1}(y)$, respectively, for all x and y,
  - when K is not known, it is computationally infeasible to compute $f_K^{-1}(y)$, even if we do know E_K.
- The algorithm E_K depends on a secret *trapdoor parameter* T such that D_K and, hence, $f_K^{-1}(y)$ is easy to find when we know T but it is computationally infeasible when we do not know T.

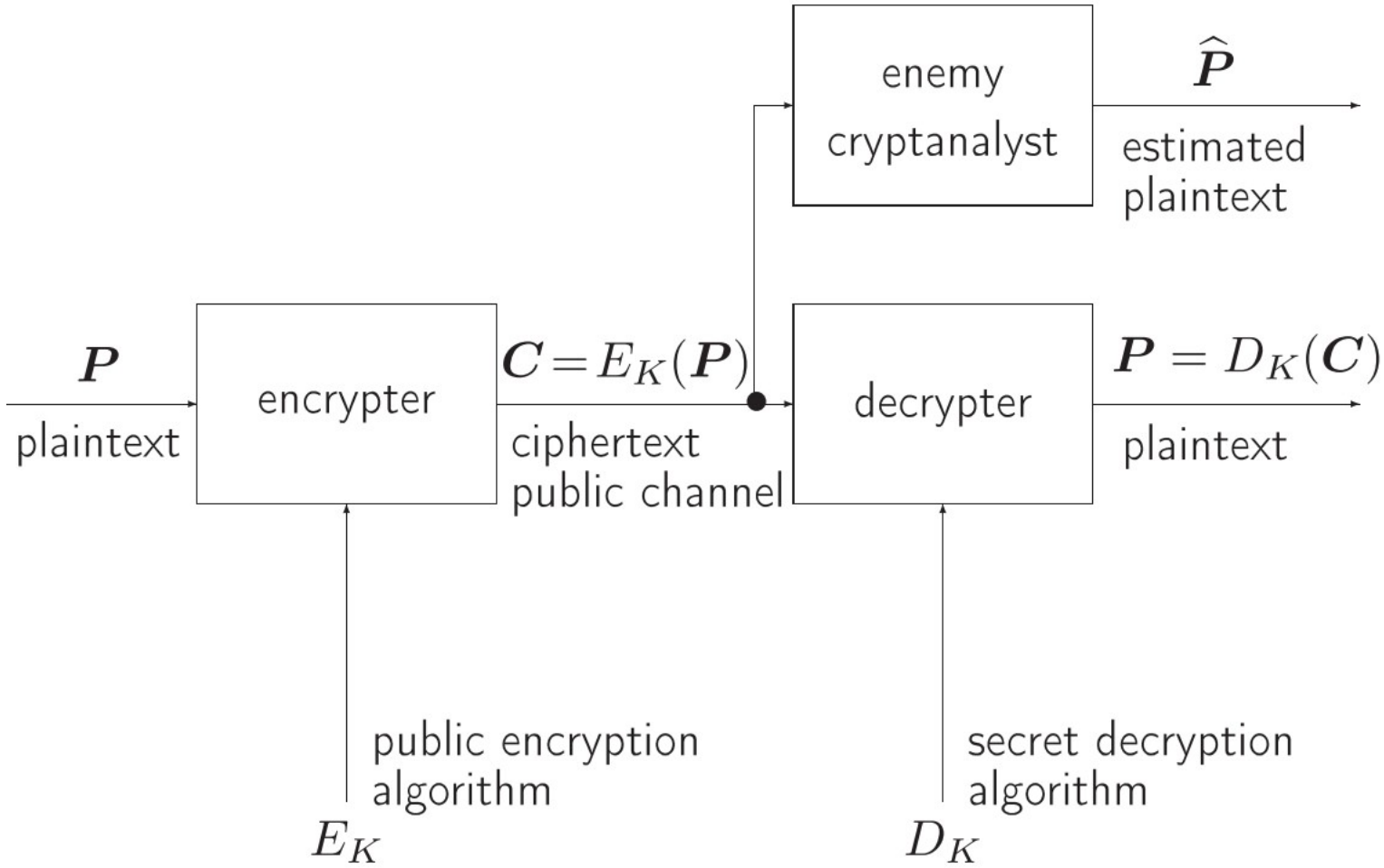
A public-key cryptosystem

Using a trapdoor one-way function we can design a so-called *two-key or public-key cryptosystem.*

Such a system can be arranged by the intended ***receiver*** (!) of encrypted information as follows.

The receiver selects his trapdoor one-way algorithm E_K, keeps the trapdoor parameter T secret, but publishes openly the encryption algorithm E_K.

A public-key cryptosystem



Some background theory

Modular arithmetic

- Modular arithmetic is an arithmetic system for integers, where numbers "wrap around" upon reaching a certain value — the modulus.
- ***Congruence***: For a positive integer n, two numbers a and b are said to be congruent modulo n if their difference $a - b$ is an integer multiple of n. We denote this as

$$a \equiv b \pmod{n}$$

which implies, for some integer k,

$$a = kn + b$$

Modular arithmentic (examples)

$a \equiv b \pmod{n}$	$a = k \cdot n + b$
$2 \equiv 0 \pmod{2}$	$2 = 1 \cdot 2 + 0$
$12 \equiv 0 \pmod{4}$	$12 = 3 \cdot 4 + 0$
$13 \equiv 1 \pmod{4}$	$13 = 3 \cdot 4 + 1$
$13 \equiv 2 \pmod{11}$	$13 = 1 \cdot 11 + 2$
$-8 \equiv 7 \pmod{5}$	$-8 = -3 \cdot 5 + 7$

Greatest common divisor (gcd)

- The greatest common divisor (gcd) of two or more integers, which are not all zero, is the largest positive integer that divides each integer.

- Example: gcd(24,54) = 6, since

1, 2, 3, and 6 are all common divisors, and **6** is the greatest.

All divisors greater than 6 are unique to one of the numbers.

Integers dividing $24 = 2^3 \cdot 3$ are 1, 2, 3, 4, **6**, 8, 12

Integers dividing $54 = 2 \cdot 3^3$ are 1, 2, 3, **6**, 9, 18, 27

Euclid's algorithm to calculate gcd

Given two natural numbers n_1 and n_2, where $n_1 > n_2$. Divide continually the larger by the smaller as follows:

$$
\begin{aligned}
n_1 &= q_0 n_2 + r_0 && (\text{dividing } n_2 \text{ into } n_1)\\
n_2 &= q_1 r_0 + r_1 && (\text{dividing } r_0 \text{ into } n_2)\\
r_0 &= q_2 r_1 + r_2 && (\text{dividing } r_1 \text{ into } r_0)\\
r_1 &= q_3 r_2 + r_3 && (\text{etc.})\\
&\vdots\\
r_{i-2} &= q_i r_{i-1} + r_i\\
r_{i-1} &= q_{i+1} r_i
\end{aligned}
$$

Then r_i is the greatest common divisor of n_1 and n_2, denoted

$$.r_i = \gcd(n_1, n_2)$$

Relatively prime (coprime) numbers

- Two integers *a* and *b* are said to be relatively prime (coprime) if the only positive integer that divides both of them is 1, i.e., if their gcd(*a*,*b*) = 1.

  Consequently, any prime number that divides one does not divide the other.

Euler's totient function

Euler's totient function, denoted $\Phi(n)$, is the number of integers between 1 and n that are relatively prime with n, that is, they have no common factors with n.

General case: Given the (unique) prime factorization of n, we can calculate Euler's totient function as

$$\Phi(n) = \Phi(p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right)$$

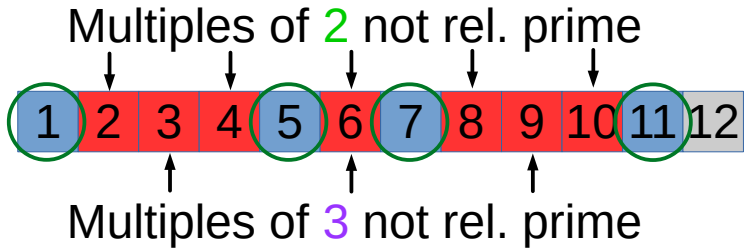
Important special case: When n is a product of two primes $n = p \cdot q$ then

$$\Phi(n) = \Phi(p \cdot q) = \Phi(p)\Phi(q) = (p-1)(q-1)$$

Euler's totient function (examples)

"General" case

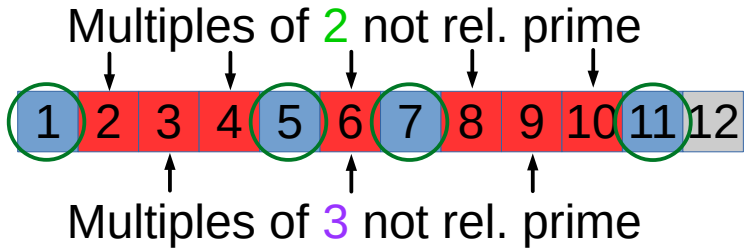
$$\Phi(12) = \Phi(2^2 3) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$$



Euler's totient function (examples)

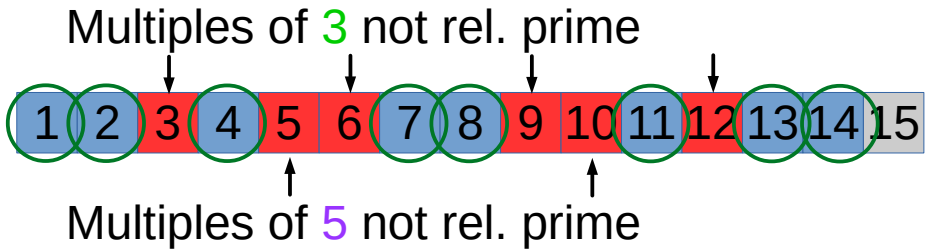
"General" case

$$\Phi(12) = \Phi(2^2 3) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$$



Special case with two primes

$$\Phi(15) = \Phi(3 \cdot 5) = (3-1) \cdot (5-1) = 8$$



A useful trapdoor one-way function

Theorem 6.2 (Euler) Let a and n be two integers that are relatively prime. Then

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{6.17}$$

or, equivalently,

$$R_n(a^{\phi(n)}) = 1 \tag{6.18}$$

where $R_d(i)$ denotes the remainder r when the integer i is divided by the divisor d, that is, $i = qd + r$, $0 \leq r < |d|$.

Bézout's identity

Given integers n_1 and n_2, not both zero, there exist integers s and t such that

$$\gcd(n_1, n_2) = sn_1 + tn_2$$

Use Euclid's algorithm backwards to find s and t

Étienne Bézout
(1730-1783)

A public-key encryption algorithm

The RSA algorithm

1. Choose two distinct prime numbers p and q.
2. Compute the product $n = pq$. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\Phi(n) = \Phi(p)\Phi(q) = (p - 1)(q - 1)$ where $\Phi()$ is Euler's totient function.
4. Choose an integer e such that $1 < e < \Phi(n)$ and $\gcd(e, \Phi(n)) = 1$; i.e., e and $\Phi(n)$ are coprime.

   The *public key* (n,e) consists of the modulus n and the public encryption exponent e

   .

   .

   .

The RSA algorithm cont.

5. Determine d as $d \equiv e^{-1} \pmod{\Phi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\Phi(n)$), i.e. solve for d given $d \cdot e \equiv 1 \pmod{\Phi(n)}$. d is kept as the private key exponent.

The *private key* (n,d) consists of the private decryption exponent d, which must be kept secret and is used together with the modulus n to calculate the clear text.
The parameters p, q, and $\Phi(n)$ must also be kept secret because they can be used to calculate d.

RSA encryption

- Alice transmits her public key (*n, e*) to Bob and keeps the private key (*n*, *d*) secret (or, more precisely, the decryption exponent *d* part of it).
- Bob wishes to send a message *p* to Alice. He first turns *p* into an integer *P*, such that $0 \leq P < n$. He then computes the cipher text *C* corresponding to $C = P^e \pmod{n}$
- Bob then transmits *C* to Alice.

RSA decryption

- Alice can recover *P* from *C* by using her private key exponent *d* via computing $P \equiv C^d \pmod{n}$
- Given *P*, Alice can recover the original message *p.*

Since an essentially larger amount of computation is involved in a two-key crypto system than in a comparably secure single-key crypto system, two-key crypto systems are mainly used in hybrid systems, where the two-key system is used to transmit a key for a single-key system used to encrypt/decrypt the main message.

Conclusion

Everybody can look up the public parameters n and e, but only those who know at least one of the secret parameters p,q, and d that are included in the trapdoor parameter T can decrypt.

If the enemy cryptanalyst, however, can factor n, then he can easily compute $\Phi(n)$ and obtain the secret decryption exponent d, and, hence, obtain the plain text.

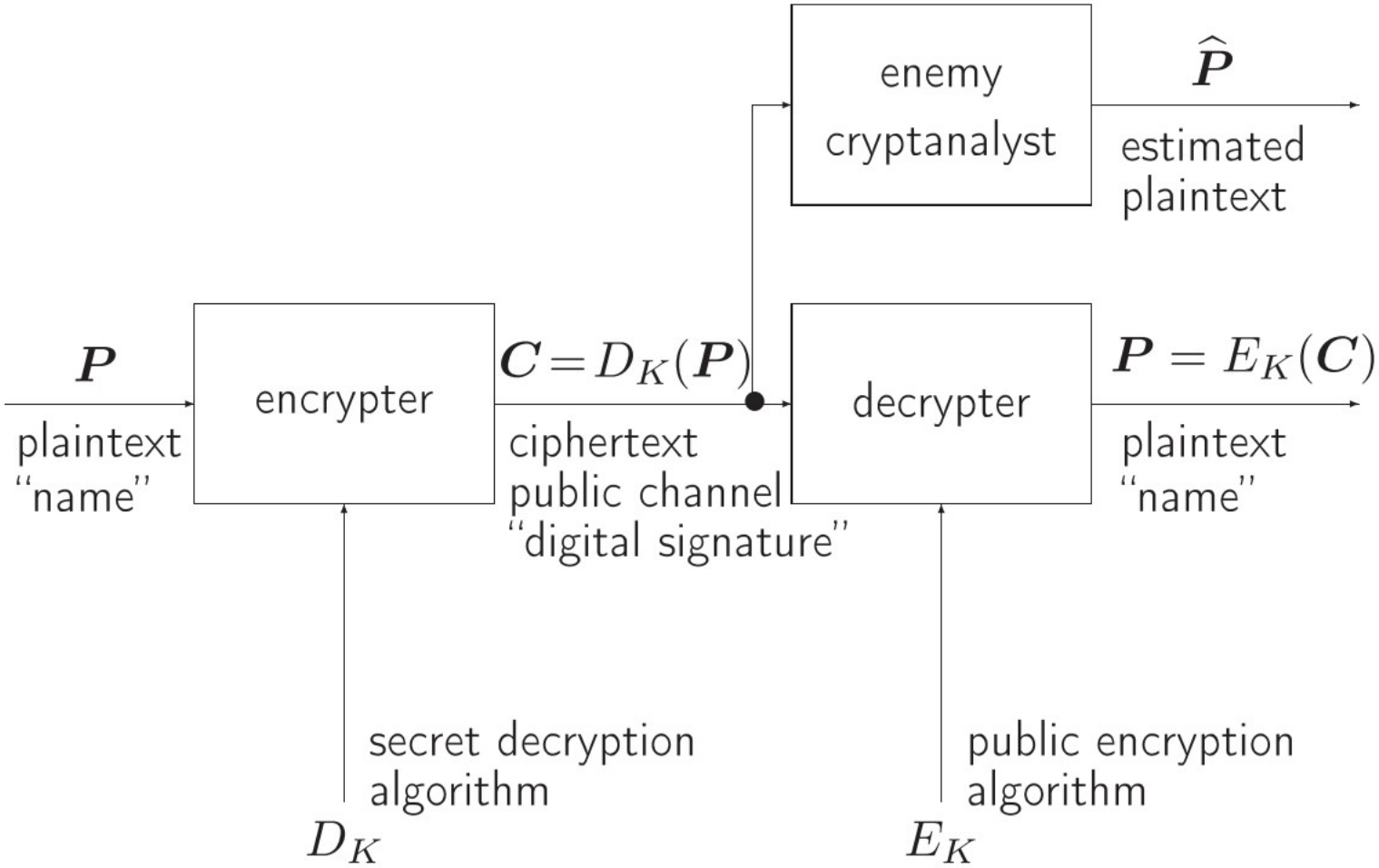
Digital signatures

A trapdoor one-way function can be used to identify a sender - to obtain a *digital signature* - but at the expense of giving up secrecy.

The *sender* who would like to create an unforgeable digital signture uses his *secret* algorithm D_K and creates a ciphertext by using, for example, his name as plaintext.

Anybody can use the senders *public* algorithm E_K to decrypt the ciphertext, and, hence, recover the sender's plaintext.

Digital signatures



Summary

- Trapdoor one-way functions are useful in cryptography, since they are somple to calculate, but very difficult to invert, unless you know the trapdoor parameter
- Public-key krypto systems are assymmetric and use two keys, one secret for decryption and one public for encryption. Everyone can encrypt, but only the one who knows the secret key can decrypt.
- Modular arithmetic, greatest common divisor, Euler's algorithm, prime/co-prime numbers, Euler's totient function, and Bézout's identity are all central key components of public-key crypto systems
- The RSA algorithms is the most well-known public-key crypto system and its security relies on the difficulty of factorizing numbers with only large prime factors
- Public-key crypto systems can also be used for digital signatures, at the cost of giving up secrecy

LUND
UNIVERSITY