Lesson 6
Introduction to cryptography

Unit 1
Symmetric ciphers

Symmetric cipher

DEFINITION (symmetric cipher)

A **symmetric cipher** is a 5-uple $(\mathcal{K}, \mathcal{M}, \mathcal{C}, e, d)$ where

$\mathcal{K}$: space of keys $\quad$ $\mathcal{M}$: space of messages $\quad$ $\mathcal{C}$: space of ciphertexts

encryption function

$$e : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$$

decryption function

$$d : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$

SYMMETRY: same key for encyption and decryption

$$\forall k \in \mathcal{K} \qquad \forall m \in \mathcal{M}$$

$$d(k, e(k, m)) = m$$

We often write $e_k(m)$ instead of $e(k, m)$, $d_k(c)$ instead of $d(k, c)$

$$d_k(e_k(m)) = m$$

Symmetric ciphers

KIRCHOFF'S PRINCIPLE

It is always better to assume that e, d are publicly known (Eve knows them).

What Eve does not know is the key.

KIRCHOFF'S PRINCIPLE

The security of a symmetric cryptosystem should depend only on the secrecy of the key, not on the secrecy of the encryption itself.

Symmetric ciphers

SUCCESSFUL CIPHERS

DEFINITION A symmetric cipher $(\mathcal{K}, \mathcal{M}, \mathcal{C}, e, d)$ is successful if:

1. $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$ it is "easy" to compute $e_k(m)$.

2. $\forall k \in \mathcal{K}, \forall c \in \mathcal{C}$ it is "easy" to compute $d_k(c)$.

3. $\forall k \in \mathcal{K}, \forall c_1, ..., c_n \in \mathcal{C}$ it is "very difficult" to obtain $m_1 = d_k(c_1), ..., m_n = d_k(c_n)$ without knowing k.

the meaning of easy/difficult will be clarified

GIVEN one or more ciphertexts it is difficult to compute the plaintext without knowing the key

⇑

4 is more restrictive than 3

4. $\forall k \in \mathcal{K}, \forall m_1, ..., m_n \in \mathcal{M}$, $\forall c \in \mathcal{C} \setminus \{c_1 = e_k(m_1), ..., c_n = e_k(m_n)\}$, knowing $(m_1, c_1), ..., (m_n, c_n)$ it is "very difficult" to find $d_k(c)$.

SECURITY AGAINS A KNOWN PLAINTEXT ATTACK

GIVEN one or more pairs of plaintexts and ciphertexts it is difficult to decrypt any ciphertext c not in the list without knowing the key

Symmetric ciphers

SUCCESSFUL CIPHERS

EXAMPLE

Which properties are fulfilled by:

a) Substitution ciphers?

1 2 3

b) De Vigenère ciphers?

1 2 3

1. $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$ it is "easy" to compute $e_k(m)$.

2. $\forall k \in \mathcal{K}, \forall c \in \mathcal{C}$ it is "easy" to compute $d_k(c)$.

3. $\forall k \in \mathcal{K}, \forall c_1, ..., c_n \in \mathcal{C}$ it is "very difficult" to obtain $m_1 = d_k(c_1), ..., m_n = d_k(c_n)$ without knowing k.

4. $\forall k \in \mathcal{K}, \forall m_1, ..., m_n \subset \mathcal{M}$, $\forall c \in \mathcal{C} \setminus \{c_1 = e_k(m_1), ..., c_n = e_k(m_n)\}$, knowing $(m_1, c_1), ..., (m_n, c_n)$ it is "very difficult" to find $d_k(c)$.

Encoding schemes

Strings of 8 bits (1 byte) may represent $2^8 = 256$ characters

EXAMPLE ASCII

	32	00100000
(	40	00101000
)	41	00101001
,	44	00101100
.	46	00101110

1 byte

A	65	01000001
B	66	01000010
C	67	01000011
D	68	01000100
⋮	⋮	⋮
X	88	01011000
Y	89	01011001
Z	90	01011010

a	97	01100001
b	98	01100010
c	99	01100011
d	100	01100100
⋮	⋮	⋮
x	120	01111000
y	121	01111001
z	122	01111010

Table 1.10: The ASCII encoding scheme

Encoding schemes

EXAMPLE **Every natural can be expressed in binary code**

$$m_{B-1}m_{B-2}\cdots m_2m_1m_0 \longleftrightarrow m_{B-1}\cdot 2^{B-1} + \cdots + m_2\cdot 2^2 + m_1\cdot 2 + m_0$$

Convert 112

Division	Remainder (R)
112 / 2 = 56	0
56 / 2 = 28	0
28 / 2 = 14	0
14 / 2 = 7	0
7 / 2 = 3	1
3 / 2 = 1	1
1 / 2 = 0	1

112 ⟷ 1110000

Encoding schemes

EXAMPLE

Encode, using ASCII, the sentence: Bed bug.

B	e	d		b	u	g	.
66	101	100	32	98	117	103	46
01000010	01100101	01100100	00100000	01100010	01110101	01100111	00101110

Encoding schemes

DEFINITION

An encoding scheme is a (publicly known) method of converting one sort of data into another sort of data, for example, converting text into numbers.

EXAMPLE

By means of ASCII, each plaintect or ciphertext can be encoded into a sequence of bytes, and each byte can be encoded with a number from 0 to 255.

Symmetric ciphers

EXAMPLE By means of ASCII in a cipher we may choose

$$\mathcal{K} = \{k \in \mathbb{N} : \ 0 \leq k < 2^{B_\mathcal{K}}\}$$

$$\mathcal{M} = \{m \in \mathbb{N} : \ 0 \leq m < 2^{B_\mathcal{M}}\}$$

$$\mathcal{C} = \{c \in \mathbb{N} : \ 0 \leq c < 2^{B_\mathcal{C}}\}$$

In order to avoid "brute force attack" (= check every k) it is enough that $B_\mathcal{K} \geq 80$

Unit 2
Examples of symmetric ciphers

Addition modulo p

EXAMPLE p big, say $p \sim 2^{160}$. Avoid brute force attacks $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{Z}/p\mathbb{Z}$

Alice and Bob randomly select secretly a key $k \in \mathcal{K} = \mathbb{Z}/p\mathbb{Z}$.

$$e_k : \mathcal{M} = \mathbb{Z}/p\mathbb{Z} \to \mathcal{C} = \mathbb{Z}/p\mathbb{Z}$$

$$\forall m \in \mathcal{M} = \mathbb{Z}/p\mathbb{Z} \qquad e_k(m) := k + m.$$

$$\forall m \in \mathcal{C} = \mathbb{Z}/p\mathbb{Z} \qquad d_k(m) := m - k.$$

Caesar's shift (p=26)

1. $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$ it is "easy" to compute $e_k(m)$.
2. $\forall k \in \mathcal{K}, \forall c \in \mathcal{C}$ it is "easy" to compute $d_k(c)$.
3. $\forall k \in \mathcal{K}, \forall c_1, ..., c_n \in \mathcal{C}$ it is "very difficult" to obtain $m_1 = d_k(c_1), ..., m_n = d_k(c_n)$ without knowing k.
4. $\forall k \in \mathcal{K}, \forall m_1, ..., m_n \in \mathcal{M}$, $\forall c \in \mathcal{C} \setminus \{c_1 = e_k(m_1), ..., c_n = e_k(m_n)\}$, knowing $(m_1, c_1), ..., (m_n, c_n)$ it is "very difficult" to find $d_k(c)$.

Known plaintext attack

Multiplication modulo p in $\mathbb{Z}/p\mathbb{Z}$

EXAMPLE p **big, say** $p \sim 2^{160}$.

Avoid brute force attacks

$$\mathcal{K} = (\mathbb{Z}/p\mathbb{Z})^* \qquad \mathcal{M} = \mathcal{C} = \mathbb{Z}/p\mathbb{Z}$$

Alice and Bob randomly select secretly a key $k \in \mathcal{K} = (\mathbb{Z}/p\mathbb{Z})^*$.

$$e_k : \mathcal{M} = \mathbb{Z}/p\mathbb{Z} \to \mathcal{C} = \mathbb{Z}/p\mathbb{Z}$$

$$\forall m \in \mathcal{M} = \mathbb{F}_p \qquad e_k(m) := k \cdot m$$

$$d_k : \mathcal{C} = Z/p\mathbb{Z} \to \mathcal{M} = \mathbb{Z}/p\mathbb{Z}$$

$$\forall c \in \mathcal{C} = \mathbb{Z}/p\mathbb{Z} \quad d_k(c) = k^{-1} \cdot c$$

1. $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$ it is "easy" to compute $e_k(m)$.
2. $\forall k \in \mathcal{K}, \forall c \in \mathcal{C}$ it is "easy" to compute $d_k(c)$.
3. $\forall k \in \mathcal{K}, \forall c_1, ..., c_n \in \mathcal{C}$ it is "very difficult" to obtain $m_1 = d_k(c_1), ..., m_n = d_k(c_n)$ without knowing k.
4. $\forall k \in \mathcal{K}, \forall m_1, ..., m_n \in \mathcal{M}$, $\forall c \in \mathcal{C} \setminus \{c_1 = e_k(m_1), ..., c_n = e_k(m_n)\}$, knowing $(m_1, c_1), ..., (m_n, c_n)$ it is "very difficult" to find $d_k(c)$.

Known plaintext attack (p is known)

Multiplication in $\mathbb{N}$

Consider now $m \mapsto e_k(m) = k \cdot m$ in $\mathbb{N}$ (instead of $\mathbb{Z}/p\mathbb{Z}$)

Reduction modulo p has a "mixing effect" that destroys divisibility

1. $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$ it is "easy" to compute $e_k(m)$.
2. $\forall k \in \mathcal{K}, \forall c \in \mathcal{C}$ it is "easy" to compute $d_k(c)$.
3. $\forall k \in \mathcal{K}, \forall c_1, ..., c_n \in \mathcal{C}$ it is "very difficult" to obtain $m_1 = d_k(c_1), ..., m_n = d_k(c_n)$ without knowing k.
4. $\forall k \in \mathcal{K}, \forall m_1, ..., m_n \in \mathcal{M}$, Known plaintext attack
$\forall c \in \mathcal{C} \setminus \{c_1 = e_k(m_1), ..., c_n = e_k(m_n)\}$, knowing $(m_1, c_1), ..., (m_n, c_n)$ it is "very difficult" to find $d_k(c)$.

EXAMPLE $c_1 = 106891 = k \cdot m_1, c_2 = 138420 = k \cdot m_2, c_3 = 569060 = k \cdot m_3,$
$c_4 = 621352 = k \cdot m_4.$

Multiplication in $\mathbb{N}$

EXAMPLE 

Bob and Alice use a cryptosystem in which their private key is a large prime k and their plaintexts and ciphertexts are integers.

Bob encrypts a message m by computing the product $c = km$. Eve intercepts the two following ciphertexts:

$$c_1 = 12849217045006222, \qquad c_2 = 6485880443666222.$$

Use the GCD method to find Bob and Alice's private key.

Affine ciphers

p **big, say** $p \sim 2^{160}$. $\quad \mathcal{M} = \mathcal{C} = \mathbb{Z}/p\mathbb{Z}$

$$\mathcal{K} = (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}/p\mathbb{Z} \qquad k = (k_1, k_2) \in \mathcal{K}$$

$$\forall m \in \mathcal{M} \quad e_k(m) = k_1 \cdot m + k_2 \qquad \forall c \in \mathcal{C} \quad d_k(c) = k_1^{-1} \cdot (c - k_2)$$

1. $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$ **it is "easy" to compute** $e_k(m)$.

2. $\forall k \in \mathcal{K}, \forall c \in \mathcal{C}$ **it is "easy" to compute** $d_k(c)$.

3. $\forall k \in \mathcal{K}, \forall c_1, \ldots, c_n \in \mathcal{C}$ **it is "very difficult" to obtain** $m_1 = d_k(c_1), \ldots, m_n = d_k(c_n)$ **without knowing** k.

4. $\forall k \in \mathcal{K}, \forall m_1, \ldots, m_n \in \mathcal{M}$,
$\forall c \in \mathcal{C} \setminus \{c_1 = e_k(m_1), \ldots, c_n = e_k(m_n)\}$, **knowing** $(m_1, c_1), \ldots, (m_n, c_n)$ **it is "very difficult" to find** $d_k(c)$.

Affine ciphers

EXAMPLE

1) Encode the alphabet from 0 to 25

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

2) Encode the plaintext “sparky”

s p a r k y

3) $p = 26, k = (3, 5) \in (\mathbb{Z}/26\mathbb{Z})^* \times \mathbb{Z}/26\mathbb{Z}$ $\quad e_k(m) = 3m + 5$

Ciphertext:

Affine ciphers

EXAMPLE In $\mathbb{Z}/26\mathbb{Z}$:

The function 9m+2 was used to obtain the ciphertext KMI. Find the plaintext.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Affine ciphers

$e_{(k_1,k_2)}(m) = k_1 \cdot m + k_2$. **How about taking** k_1 **non invertible in** $\mathbb{Z}/p\mathbb{Z}$**?**

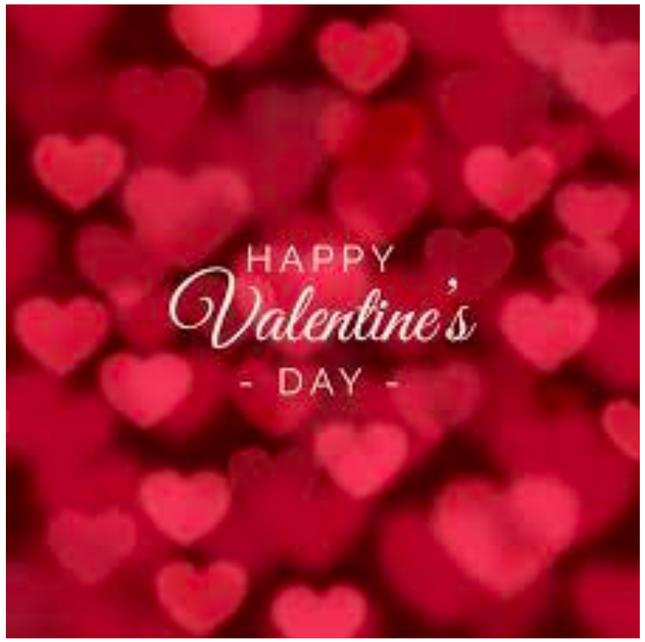
EXAMPLE

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Consider $e(m) = 13m + 5$ **in** $\mathbb{Z}/26\mathbb{Z}$.

1) Encrypt “love”

2) Encrypt “hate”



Stream cipher: Exclusive OR (XOR)

ONE BIT AT A TIME

XOR is nothing more than the sum in $\mathbb{Z}/2\mathbb{Z}$

DEFINITION (XOR)

$$\text{If } a, b \in \{0,1\} \text{ we define} \quad a \oplus b = \begin{cases} 0 & \text{if } a = b, \\ 1 & \text{if } a \neq b. \end{cases}$$

$$\text{If } a_1 \ldots a_n,\ b_1 \ldots b_n \text{ are two binary strings we set}$$

$$a_1 \ldots a_n \oplus b_1 \ldots b_n = (a_1 \oplus b_1) \ldots (a_n \oplus b_n)$$

EXAMPLE $10110 \oplus 11010 =$

EXAMPLE $\forall a \in \{0,1\}^n \quad a \oplus a = 00 \ldots 0$

XOR cipher

$$B \geq 1,\ \mathcal{K} = \mathcal{M} = \mathcal{C} = \{k \in \mathbb{N} :\ 0 \leq k < 2^B\}$$

$$\forall k \in \mathcal{K},\ \forall m \in \mathcal{M} \qquad e_k(m) = k \oplus m$$

$$\forall c \in \mathcal{C} \quad d_k(c) = k \oplus c = e_k(c)$$

1. $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$ it is "easy" to compute $e_k(m)$.

2. $\forall k \in \mathcal{K}, \forall c \in \mathcal{C}$ it is "easy" to compute $d_k(c)$.

3. $\forall k \in \mathcal{K}, \forall c_1, ..., c_n \in \mathcal{C}$ it is "very difficult" to obtain $m_1 = d_k(c_1), ..., m_n = d_k(c_n)$ without knowing k.

4. $\forall k \in \mathcal{K}, \forall m_1, ..., m_n \in \mathcal{M}$, $\forall c \in \mathcal{C} \setminus \{c_1 = e_k(m_1), ..., c_n = e_k(m_n)\}$, knowing $(m_1, c_1), ..., (m_n, c_n)$ it is "very difficult" to find $d_k(c)$.

EXAMPLE $c = 100101,\ m = 001101$: find k.

If k is chosen randomly and used once , it is known as Vernan's one-time pad

Block ciphers: Hill cipher

ONE BLOCK AT A TIME

p prime. $\quad e_k(m) = k_1 \cdot m + k_2$

k_1 invertible $n \times n$ matrix in $\mathbb{F}_p$

m, k_2 vectors in $(\mathbb{F}_p)^n$

m: block of n plain letters/numbers

EXAMPLE

Use Hill cipher with $p = 13$, matrix $k_1 = \begin{pmatrix} 5 & 7 \\ 8 & 4 \end{pmatrix}$, $k_2 = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$ to encrypt $m = \begin{pmatrix} 3 \\ 7 \end{pmatrix}$.

Block ciphers: Hill cipher

EXAMPLE Use Hill cipher with $p = 29$, matrix $k_1 = \begin{pmatrix} 3 & 2 \\ 12 & 9 \end{pmatrix}$ and $k_2 = 0$ to encrypt "hill".

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	,	?
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

h i l l

Block ciphers: Hill cipher

EXAMPLE

A Hill cipher with $p = 31$, matrix $k_1 = \begin{pmatrix} 11 & 2 \\ 12 & 3 \end{pmatrix}$ and $k_2 = 0$ was used to encrypt a message.

The ciphertext is $8 - 13 - 21 - 14$. What is the plaintext?

An alternative with matrices

LEMMA (Determinants modulo p) Let $p =$ be prime.

Let A be a $n \times n$ matrix in $\mathbb{Z}/p\mathbb{Z}$ and $B \in (\mathbb{Z}/p\mathbb{Z})^n$.
If $\det(A)$ is invertible in $\mathbb{Z}/p\mathbb{Z}$ then A has an inverse A^{-1} in $\mathbb{Z}/p\mathbb{Z}$ and the equation $AU = B$ has exactly one solution $U \in (\mathbb{Z}/p\mathbb{Z})^n$, given by $U = A^{-1}B$.

In dimension 2:

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \qquad A^{-1} = (\det A)^{-1} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

Block ciphers: Hill cipher

EXAMPLE

A Hill cipher with $p = 31$, matrix $k_1 = \begin{pmatrix} 11 & 2 \\ 12 & 3 \end{pmatrix}$ and $k_2 = 0$ was used to encrypt a message.

The ciphertext is $8 - 13 - 21 - 14$. What is the plaintext?

Block ciphers

The block ciphers that are used for situations where security is important use bigger blocks and are faster than Hill ciphers. One of the most widely used block ciphers was DES (Data Encryption Standard), which was invented in the 1970s (IBM) and was the standard cryptographic block cipher for more than 25 years. It used plaintext blocks of 64 bits and produced ciphertext blocks also of 64 bits; still used.

Block ciphers

In 2001, AES (Advanced Encryption Standard) was introduced as a replacement for DES. It uses blocks of 128 bits. Both DES and AES are widely used in Internet commerce.

Unit 3
Asymmetric ciphers

Non mathematical formulation

Bob

encryption using the public key (putting in the safe)

The safe: public key

Alice

The key/code to open the safe: the private key

Asymmetric cipher

DEFINITION (asymmetric cipher)

An **asymmetric cipher** is a 5-uple $(\mathcal{K}, \mathcal{M}, \mathcal{C}, e, d)$ where

$\mathcal{K} \subset \mathcal{K}_{\text{priv}} \times \mathcal{K}_{\text{pub}}$: space of keys

$\mathcal{K}_{\text{priv}}$: private keys

$\mathcal{K}_{\text{pub}}$: public keys

$\mathcal{M}$: space of messages

$\mathcal{C}$: space of ciphertexts

encryption function

$$e : \mathcal{K}_{\text{pub}} \times \mathcal{M} \to \mathcal{C}$$

decryption function

$$d : \mathcal{K}_{\text{priv}} \times \mathcal{C} \to \mathcal{M}$$

$$\forall (k_{\text{priv}}, k_{\text{pub}}) \in \mathcal{K} \qquad \forall m \in \mathcal{M} \qquad \boxed{d(k_{\text{priv}}, e(k_{\text{pub}}, m)) = m}$$

We often write $e_{k_{\text{pub}}}(m)$ instead of $e(k_{\text{pub}}, m)$, $d_{k_{\text{priv}}}(c)$ instead of $d(k_{\text{priv}}, c)$

$$\boxed{d_{k_{\text{priv}}}(e_{k_{\text{pub}}}(m)) = m}$$

Asymmetric ciphers

SUCCESSFUL CIPHERS

DEFINITION An asymmetric cipher $(\mathcal{K}, \mathcal{M}, \mathcal{C}, e, d)$ $(\mathcal{K} \subset \mathcal{K}_{\text{priv}} \times \mathcal{K}_{\text{pub}})$ is successful if:

1. $\forall k_{\text{pub}} \in \mathcal{K}_{\text{pub}}, \forall m \in \mathcal{M}$ it is "easy" to compute $e_{\text{pub}}(m)$.

2. $\forall k_{\text{priv}} \in \mathcal{K}_{\text{priv}}, \forall c \in \mathcal{C}$ it is "easy" to compute $d_{\text{priv}}(c)$.

3. Knowing $k_{\text{pub}} \in \mathcal{K}_{\text{pub}}$ and $c_1, ..., c_n \in \mathcal{C}$ it is difficult to compute $m_1 = d_{k_{\text{priv}}}(c_1), ..., m_n = d_{k_{\text{priv}}}(c_n)$.

4. $\forall k_{\text{pub}} \in \mathcal{K}_{\text{pub}}$, $\forall k_{\text{priv}} \in \mathcal{K}_{\text{priv}}$
$\forall m_1, ..., m_n \in \mathcal{M}$, $\forall c \in \mathcal{C} \setminus \{c_1 := e_{k_{\text{pub}}}(m_1), ..., c_n := e_{k_{\text{pub}}}(m_n)\}$,
knowing $(m_1, c_1), ..., (m_n, c_n)$ it is "very difficult" to find $d_{k_{\text{priv}}}(c)$.

SECURITY AGAINS A KNOWN PLAINTEXT ATTACK

REMARK 3. $\Rightarrow$ Alice can send k_{pub} to Bob and Bob can send back the ciphertext $e_{k_{\text{pub}}}(m)$ using an insecure communication.

Symmetric/asymmetric

Symmetric ciphers

SUCCESSFUL CIPHERS

DEFINITION A symmetric cipher $(\mathcal{K}, \mathcal{M}, \mathcal{C}, e, d)$ is successful if:

1. $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$ it is "easy" to compute $e_k(m)$.
2. $\forall k \in \mathcal{K}, \forall c \in \mathcal{C}$ it is "easy" to compute $d_k(c)$.
3. $\forall k \in \mathcal{K}, \forall c_1, ..., c_n \in \mathcal{C}$ it is "very difficult" to obtain $m_1 = d_k(c_1), ..., m_n = d_k(c_n)$ without knowing k.
4. $\forall k \in \mathcal{K}, \forall m_1, ..., m_n \in \mathcal{M}$, $\forall c \in \mathcal{C} \setminus \{c_1 = e_k(m_1), ..., c_n = e_k(m_n)\}$, knowing $(m_1, c_1), ..., (m_n, c_n)$ it is "very difficult" to find $d_k(c)$.

Asymmetric ciphers

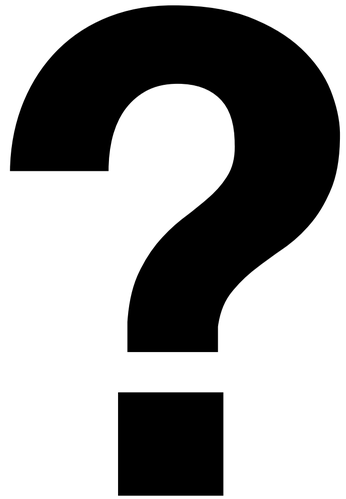
SUCCESSFUL CIPHERS

DEFINITION An asymmetric cipher $(\mathcal{K}, \mathcal{M}, \mathcal{C}, e, d)$ $(\mathcal{K} \subset \mathcal{K}_{priv} \times \mathcal{K}_{pub})$ is successful if:

1. $\forall k_{pub} \in \mathcal{K}_{pub}, \forall m \in \mathcal{M}$ it is "easy" to compute $e_{pub}(m)$.
2. $\forall k_{priv} \in \mathcal{K}_{priv}, \forall c \in \mathcal{C}$ it is "easy" to compute $d_{priv}(c)$.
3. Knowing $k_{pub} \in \mathcal{K}_{pub}$ and $c_1, ..., c_n \in \mathcal{C}$ it is difficult to compute $m_1 = d_{k_{priv}}(c_1), ..., m_n = d_{k_{priv}}(c_n)$.
4. $\forall k_{pub} \in \mathcal{K}_{pub}$, $\forall k_{priv} \in \mathcal{K}_{priv}$ $\forall m_1, ..., m_n \in \mathcal{M}$, $\forall c \in \mathcal{C} \setminus \{c_1 := e_{k_{pub}}(m_1), ..., c_n := e_{k_{pub}}(m_n)\}$, knowing $(m_1, c_1), ..., (m_n, c_n)$ it is "very difficult" to find $d_{k_{priv}}(c)$.

Asymmetric ciphers

EXAMPLE



Diffie-Hellman created the concept without finding a candidate for a pair of functions. Some asymmetric ciphers: RSA, Elgamal, Goldwasser-Mical, Elliptic Curve Cryptography, GGH, NTRU,…

END of
Lesson 6
Introduction to cryptography