Key Generation:

- Choose two large and distinct primes p,q and set $N = pq$
- Note that $\varphi(N)=(p-1)(q-1)$
- Plaintext space and ciphertext space: $\mathbb{Z}_N^*$
- Choose an exponent $e > 1$ with $gcd(e,\varphi(N)) = 1$
- Compute the unique exponent $d > 1$ with $ed \equiv 1 \pmod{\varphi(N)}$
- **Public key**: (N,e) **Secret key**: d

Hybrid encryption:

First, we use public-key encryption to exchange a secret-key, which we then use in a secret-key encryption scheme in the remaining communication.

Encryption with public key (N,e):

$c = E(m,e) = m^e \bmod N$

Decryption with secret key d:

$m = D(c,d) = c^d \bmod N$

TEXTBOOK RSA SIGNATURE: "SIGNING BY DECRYPTING"

Assume that Alice uses the public signature key (N,e) in the textbook RSA signature scheme.

Generate a valid signature $s \in \mathbb{Z}_N^*$ under Alice's private signature key on an arbitrary message $m \neq 1$, **without** using Alice's private signature key. To do so, you can choose this message m yourself (even at random, if you want), but you have to guarantee that $m \in \mathbb{Z}_N^*$, $m \neq 1$, and that you didn't use Alice's private signature key at all!

Antwoord op 6.

1. We choose an arbitrary (e.g., at random) signature $s \in \mathbb{Z}_N^*$ such that $s \neq 1$. *(5 points)*
2. Then, we compute $m = s^e \bmod N$ as our message. *(5 points)*

Key Generation:

- Choose two large primes p,q and set $N = pq$
- Note that $\varphi(N)=(p-1)(q-1)$
- Message space and signature space: $\mathbb{Z}_N^*$
- Choose an exponent $e > 1$ with $gcd(e,\varphi(N)) = 1$
- Compute the unique exponent $d > 1$ with $ed \equiv 1 \pmod{\varphi(N)}$
- **Public key**: (N,e) **Secret key**: d

Signing with secret key d:

$s = m^d \bmod N$

Verifying with public key (N,e):

check whether $m = s^e \bmod N$

If you know N, p and q. You know φ(N) = (p-1)(q-1). If you factorize the φ(N), you can get the lowest prime number where φ(N) is not dividable (gcd(e, φ(N))) =1), this is e.

Obtain secret key d:

e*d mod φ(N) = 1

Do Euclidean(e, φ(N)). This gives t,x,y. t should be equal to 1.

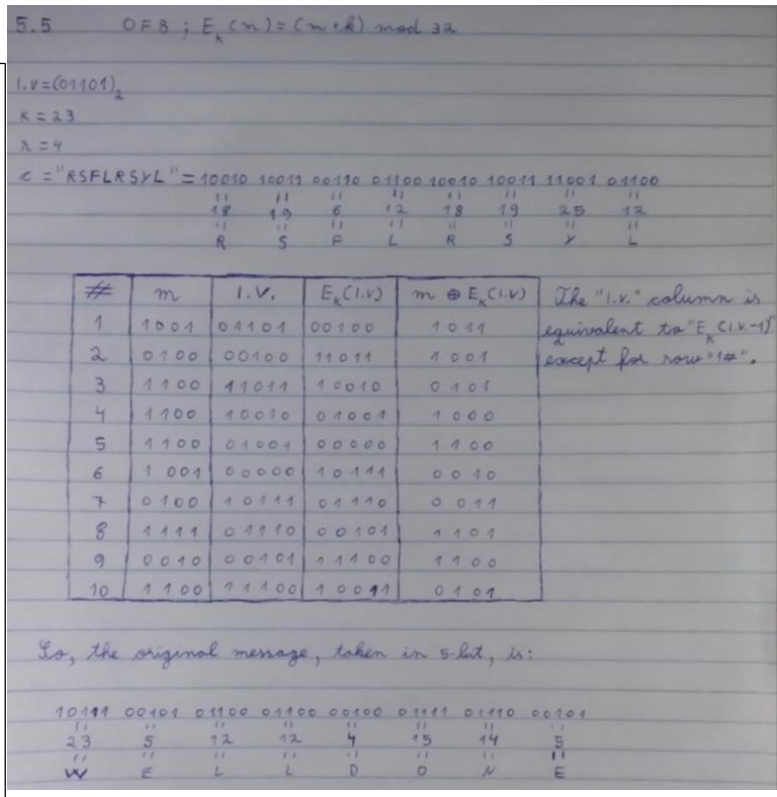
a*x+b*y = t. In our case: e*x + φ(N)*y = 1.

Go to: (e*x) mod φ(N) + (φ(N)*y) mod φ(N) = 1 mod φ(N)

You will see: (e*x) mod φ(N) + 0 = 1 mod φ(N)

D = x mod φ(N).

Now you can encrypt/decrypt any message using m,e and c,d.



5.5 OFB ; $E_K(m) = (m+K) \bmod 32$

I.V. = $(01101)_2$

K = 23

λ = 4

c = "RSFLRSYL" = 10010 10011 00110 01100 10010 10011 11001 01100

18 19 6 12 18 19 25 12

R S F L R S Y L

#	m	I.V.	E_K(I.V.)	$m \oplus E_K$(I.V.)
1	1001	01101	00100	1011
2	0100	00100	11011	1001
3	1100	11011	10010	0101
4	1100	10010	01001	1000
5	1100	01001	00000	1100
6	1001	00000	10111	0010
7	0100	10111	01110	0011
8	1111	01110	00101	1101
9	0010	00101	11100	1100
10	1100	11100	10011	0101

The "I.V." column is equivalent to "E_K(I.V.-1)" except for row "1".

So, the original message, taken in 5-bit, is:

10111 00101 01100 01100 00100 01111 01110 00101

23 5 12 12 4 15 14 5

W E L L D O N E

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

One time pad (vernam cipher)

Plaintext encoded as binary sequence $m \in \{0,1\}^n$

Secret key $k \in \{0,1\}^n$ is chosen at random

Ciphertext is computed as: $c = m$ XOR k

Key has *at least the length* of the message

Key is chosen *uniformly at random*

Key is used only *once* (→ „one time pad“)

Definition (Shannon):

A cipher is *perfectly secret / secure*, if

$P[M=m] = P[M=m|C=c]$

Probability that the plaintext is m

Probability that the plaintext is m, given that the ciphertext is c

CBC (k=11) $E_k(m) = (m+k) \mod 16,$

0	1	2	3	4	5	6	7
A	T	C	W	E	M	N	!

"TWENTE" translates into $(1,3,4,6,1,4)$.
In 3-bit binary this is: 001 011 100 110 001 100.
In blocks of length $n = 4$: 0010 1110 0110 0011 0010 (we use "padding").
We encrypt this using the notation from the first lecture:

block nr j	plaintext m_j	c_{j-1}	$m_j \oplus c_{j-1}$	c_j
1	0010	IV = 1010	$(1000)_2 = (8)_{10}$	$(3)_{10} = (0011)_2$
2	1110	0011	$(1101)_2 = (13)_{10}$	$(8)_{10} = (1000)_2$
3	0110	1000	$(1110)_2 = (14)_{10}$	$(9)_{10} = (1001)_2$
4	0011	1001	$(1010)_2 = (10)_{10}$	$(5)_{10} = (0101)_2$
5	0010	0101	$(0111)_2 = (7)_{10}$	$(2)_{10} = (0010)_2$

The bit-encryption of "TWENTE" is therefore: 0011 1000 1001 0101 0010.

ECB (k=5): $E_k(m) = (m+k) \mod 8,$

0	1	2	3
D	E	G	O

"GOED" translates into $(2,3,1,0)$.
In 2-bit binary this is: 10 11 01 00.
In blocks of length $n = 3$: 101 101 001 (we use "padding").
We encrypt this using the notation from the first lecture:

block nr j	plaintext m_j	c_j
1	$(101)_2 = (5)_{10}$	$(2)_{10} = (010)_2$
2	$(101)_2 = (5)_{10}$	$(2)_{10} = (010)_2$
3	$(001)_2 = (1)_{10}$	$(6)_{10} = (110)_2$

The bit-encryption of "GOED" is therefore: 010 010 110.

$$64^{531} \mod 121$$

We start by converting the exponent 531 into its binary representation: 1000010011. This means that

$$531 = 2^9 + 2^4 + 2^1 + 2^0.$$

By using the rules of modular arithmetic, we can hence write

$$64^{531} \mod 121 = 64^{2^9} \mod 121 \cdot 64^{2^4} \mod 121 \cdot 64^{2^1} \mod 121 \cdot 64^{2^0} \mod 121.$$

We then compute each factor separately, which yields:

$$64^{531} \mod 121 = (26 \cdot 42 \cdot 103 \cdot 64) \mod 121 = 53.$$

Keys: N*(N-1) / 2

THE EXTENDED EUCLIDEAN ALGORITHM

Input: a,b

Output: t,x,y with t=gcd(*a,b*) and *ax+by=t*

if *b=0* **then** *t=a, x=1, y=0;* **return;**
$x_2=1; x_1=0; y_2=0; y_1=1;$
while *b>0*
  $q=a$ div b; $r=a$ mod b; $x=x_2-qx_1$; $y=y_2-qy_1$;
  $a=b$; $b=r$; $x_2=x_1$; $x_1=x$; $y_2=y_1$; $y_1=y$;
end while
$t=a$; $x=x_2$; $y=y_2$;

q	r	x	y	a	b	x_2	x_1	y_2	y_1

Theorem: For integers a, a_1, b, b_1, c and $n>0$, we have:

- $a \equiv b \pmod n \Leftrightarrow a \bmod n = b \bmod n$ ("alternative definition")
- $a \equiv a \pmod n$
- If $a \equiv b \pmod n$, then $b \equiv a \pmod n$
- If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$
- If $a \equiv a_1 \pmod n$ and $b \equiv b_1 \pmod n$, then
  - $a+b \equiv a_1+b_1 \pmod n$
  - $ab \equiv a_1 b_1 \pmod n$

For all primes p: φ (p) = p-1
For N=pq with distinct primes p,q: Ψ(N) = (p-1)(q-1)

Definition: We denote the subset of $\mathbb{Z}_n = \{0,\dots,n-1\}$ that contains only elements *a* with *gcd(a,n) = 1* by $\mathbb{Z}_n^*$, i.e.

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$$

This set is called the set of **invertible elements modulo *n***.

Steganography: hide the fact there is a special message.

Cryptography: Make the message unreadable to others. But everyone can see the message.