# Cvičení 8.4.2024

- 1. Nalezněte Eulerovo číslo pro n = 26, 29, 35, 49, 600, tj. nalezněte všechna m, 1≤m<n, která jsou nesoudělná s n.
- 2. Nalezněte aditivní opačný prvek ke všem prvkům v množině celých čísel modulo m, kde m = 8, 11.
- Nalezněte multiplikativní inverzní prvek ke všem prvkům v množině celých čísel modulo m, kde m = 8, 11.
- 4. Simulujte šifrování a dešifrování pomocí RSA pokud jsou dány následující hodnoty:
  - a) p=7, q=11, e=17, m=8,
  - b) p=13, q=11, e=7, m=5,
  - c) Pro určení multiplikativního inverzního (tedy soukromého klíče) prvku použijte EEA, např. https://planetcalc.com/3311/

Cryptool: Encryption or decryption of messages using the RSA key pair.

1. Select Individual Procedures/RSA Cryptosystem/RSA Demonstration



2. Enter the RSA key p=47, q=79, e=37. The parameters  $N = p^*q=3713$  and phi(N)=3588 and d=97 are calculated.

RSA using the private	and public key or using only the public ke	y
Choose two prim (p-1)(q-1) is the E key d is then calc	e numbers p and q. The composite number N uler totient. The public key e is freely choser sulated such that d = e^(-1) (mod phi(N)).	N = pq is the public RSA modulus, and phi(N) = n but must be coprime to the totient. The private
C For data encrypti and the public ke	on or certificate verification, you will only nee ay e.	ed the public RSA parameters: the modulus N
Prime number entry		
Prime number p	47	Generate prime numbers
Prime number q	79	
- RSA parameters		
RSA modulus N	3713	(public)
phi(N) = (p-1)(q-1)	3588	(secret)
Public key e	37	
Private key d	97	Update parameters
	e / decryption using d	
RSA encryption using		
RSA encryption using	C numbers	Alphabet and number system options
RSA encryption using Input as • text Enter the message for	C numbers or encryption or decryption either as text or a	Alphabet and number system options
RSA encryption using Input as  • text Enter the message fo	C numbers or encryption or decryption either as text or a	Alphabet and number system options
RSA encryption using	C numbers or encryption or decryption either as text or a	Alphabet and number system gptions
RSA encryption using     Input as      text     Enter the message fo	C numbers or encryption or decryption either as text or a	Alphabet and number system gptions
RSA encryption using	C numbers or encryption or decryption either as text or a	Alphabet and number system gptions
RSA encryption using Input as  text Enter the message fo	C numbers or encryption or decryption either as text or a	Alphabet and number system gptions
RSA encryption using Input as  text Enter the message fo	C numbers or encryption or decryption either as text or a	Alphabet and number system gptions
RSA encryption using Input as  text Enter the message fo	C numbers or encryption or decryption either as text or a	Alphabet and number system gptions

## 3. Click Alphabet and number system options

RSA Demonstration Options
Alphabet options     All 256 ASCII characters     Specify alphabet:     All 256 ASCII characters: 256     Specify alphabet:     ABCDEEGHLIKLMNDDDBSTLINAWYZ
RSA variant © Normal C Dialogue of the Sisters
Method for coding a block into numbers
Block length The number of characters that are encrypted with each RSA operation. The maximum size of a block is limited by the bit length of the modulus N, the number of characters in the alphabet, and the encoding method. Block length in characters: 1 (Maximum block length 1 characters)
Number system           The numbers for encryption and decryption will be represented in the following radix:                • Decimal                 • Decimal

4. Choose specify alphabet under Alphabet Options and number system under Method for coding of text into number. Enter 2 in Block length in characters.

Iphabet options C All 256 <u>A</u> SCII characte Specify alphabet:	rs Number of characters: 27
ABCDEFGHIJKLMNO	PQRSTUVWXYZ
ISA variant	
• <u>N</u> ormal C	Dialogue of the <u>S</u> isters
1ethod for coding a block ir	nto numbers
C b-adjc •	N <u>u</u> mber system
lock length	
The number of characters The maximum size of a blo number of characters in the	that are encrypted with each RSA operation. ck is limited by the bit length of the modulus N, the e alphabet, and the encoding method.
Block length in characters:	2 (Maximum block length 2 characters)
lumber system	
The numbers for encryptio following radix:	n and decryption will be represented in the
Decimal	Binary COctal CHexadecimal

5. To confirm your entries, click on OK. You can now enter the input the text, "WORKSHOP AT CHATTANOOGA", in the input line and click on the Encrypt button.

(p-1) (q-1) is the E key d is then calc	<ul> <li>numbers p and q. The composite number N = uler totient. The public key e is freely chosen bu ulated such that d = e<sup>-</sup>(-1) (mod phi(N)).</li> </ul>	pq is the public hisk modulus, and phills i ut must be coprime to the totient. The priva
<ul> <li>For data encryption and the public ket</li> </ul>	on or certificate verification, you will only need t y e.	the public RSA parameters: the modulus N
Prime number entry —		
Prime number p	47	Generate prime numbers.
Prime number q	79	
RSA parameters		
RSA modulus N	3713	(public)
phi(N) = (p-1)(q-1)	3588	(secret)
Public keye	37	
D:	97	Update parameters
Private Key d	Jul 201	
Private Key d	e / decruption using d	
Private Key d RSA encryption using	e / decryption using d	Alphabet and number system options
Private Key d RSA encryption using Input as I text	e / decryption using d	Alphabet and number system gptions
Private key d RSA encryption using Input as  (* text Input text	e / decryption using d	Alphabet and number system <u>options</u>
Private key d RSA encryption using Input as retext Input text WORKSHOP AT CH The Input text will be	e / decoption using d  c numbers IATTANOOGA seconded into seconents of Size 2 filte symbol	Alphabet and number system options
Private Key d RSA encryption using Input as retext Input text WORKSHOP AT CH The Input text will be WO # RK # SH # 0	P  P  P  P  P  P  P  P  P  P  P  P  P	Alphabet and number system gptions #/ is used as separator).
Private Key d RSA encryption using Input as retext Input text WORKSHOP AT CH The Input text will be WO # RK # SH # 0 Numbers input in bas		Alphabet and number system gptions
Private Key d RSA encryption using Input as retxt Input text WORKSHOP AT CF The Input text will be WO # RK # SH # 0 Numbers input in bas 2315 # 1811 # 1908	e / decryption using d	Alphabet and number system gptions # is used as separator). 1 # 1415 # 1507 # 0100
Private key d RSA encryption using Input as • text Input text WORKSHOP AT CH The Input text will be WO # RK # SH # 0 Numbers input in bas [2315 # 1811 # 1908 Encruption ido ciba	p**           e / decryption using d           C numbers           LATTANDOGA           separated into segments of Size 2 (the symbol           P # A # T # CH # AT # TA # NO # 0 G # A           e 10 format           # 1516 # 00001 # 2000 # 0308 # 0120 # 200*           uter cfD = ord/D = forced N	Alphabet and number system <u>options</u> W is used as separator).
Private key d RSA encryption using Input as  text Input text [VOBRSHOP AT CF The Input text will be [VOB #K # SH # 0 Numbers input in bes [2315 # 1811 # 1900 Encryption into ciphe [1999 # 2301 # 254	p"         p"           e / decryption using d	Alphabet and number system gptions #* is used as separator). 1 # 1415 # 1507 # 0100 2 # 0006 # 1006

6. To decrypt, copy text in Encryption into ciphertext 1999 # 3408 # 2545 #

2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 to input text area. And click Decrypt button.

RSA Demonstration			<b>×</b>
RSA using the private     C Choose two prime     (p-1)(q-1) is the Eu     key d is then calculated of the calculated of the public key     and the public key	and public key or using only the numbers p and q. The composituler tolient. The public key e is fre ulated such that d = e^[-1] (mod p n or certificate verification, you w y e.	: public key mumber N = pq is the public RSA mode elv chosen but must be coprime to the t hi(N)). ill only need the public RSA parameters	ulus, and phi(N) = otient. The private : the modulus N
Prime number entry-			
Prime number p	47	Generate	prime numbers
Prime number q	79		
RSA parameters			
RSA modulus N	3713	(public)	
phi(N) = (p-1)(q-1)	3588	(secret)	
Public keye	37		
Private key d	97	<u>U</u> pda	te parameters
- RSA encryption using	e / decryption using d		
Input as C text	• numbers	Alphabet and number sy:	stem options
Ciphertext coded in n	umbers of base 10		
1999 # 3408 # 2545	# 2798 # 0001 # 3284 # 3613 #	1404 # 2932 # 0208 # 1095 # 3306	
Decryption into plaint	ext m[i] = c[i]^d (mod N)		
2315 # 1811 # 1908	# 1516 # 0001 # 2000 # 0308 #	0120 # 2001 # 1415 # 1507 # 0100	
Output text from the c	lecryption (into segments of size 2	; the symbol '#' is used as separator).	
WO # RK # SH # O	P # A # T # CH # AT # TA # N	D # 0G # A	
Plaintext			
WORKSHOP AT CH	ATTANOOGA		
Encrypt	Decrypt		<u>C</u> lose

Cryptool: Encryption of the message with block length 1 v.s. encryption of the message with block length 2.

-

1. Create the RSA key p=251, q=269, e=65537.

15A using the private	and public key or using only the public key	
Choose hup prime	and public Key - of dailing only the public Key	- og is the public RSA modulus, and phißt) -
(p-1)(q-1) is the E key d is then calc	uler totient. The public key e is freely chosen ulated such that d = e^(-1) (mod phi(N)).	but must be coprime to the totient. The privat
C For data encryption and the public keep	on or certificate verification, you will only nee y e.	d the public RSA parameters: the modulus N
<sup>p</sup> rime number entry —		
Prime number p	251	Generate prime numbers.
Prime number q	269	
RSA parameters		
RSA modulus N	67519	(public)
phi(N) = (p-1)(q-1)	67000	(secret)
Public key e	65537	
Private key d	2473	Update parameters
RSA encryption using	e / decryption using d	
	C numbers	Alphabet and number system gptions
Input as 📀 itext		
Input as  • text Enter the message for	r encryption or decryption either as text or as	hex dump.
Input as  • lext Enter the message fo	r encryption or decryption either as text or as	hex dump.
Input as (* text Enter the message fo	r encryption or decryption either as text or as	hex dump.
Input as • text	r encryption or decryption either as text or as	hex dump.
Input as related Enter the message fo	r encryption or decryption either as text or as	hex dump.
Input as related to the message for	r encryption or decryption either as text or as	hex dump.
Input as related	r encryption or decryption either as text or as	hex dump.
Input as related	r encryption or decryption either as text or as	hex dump.

2. Click Alphabet and number system options

Choose All 256 ASCII characters under Alphabet options, b-adic under Method for coding and a block into numbers and 1 in Block length in characters.

Alphabet options -	characters abet:	Number of chara	cters: 256
ABCDEFGH	IJKLMNOPQRSTUV	WXYZ	
RSA variant			
	C Dialogue o	if the <u>S</u> isters	
Method for coding	a block into number	\$	
● b-adjc	C Number sy	stem	
Block length			
The number of c The maximum siz number of chara	haracters that are en e of a block is limited cters in the alphabet,	icrypted with each R d by the bit length of , and the encoding ri	SA operation. the modulus N, the nethod.
Block length in c	haracters: 1	(Maximum block len	gth 2 characters)
Number system			
The numbers for	encryption and deci	yption will be represe	ented in the
following radix:	12111111	0.011	C Hexadecimal
following radix:	C <u>B</u> inary	Uctai	Touggooma

3. To confirm your entries, click on OK. You can now enter the input the text, "RUBY FALLS!", in the input line and click on the Encrypt button.

13A using the private	and public key - or using only the public key -	
Choose two prime (p-1)(q-1) is the E key d is then calc	<ul> <li>numbers p and q. The composite number N = uler totient. The public key e is freely chosen bu ulated such that d = e<sup>-</sup>(-1) (mod phi(N)).</li> </ul>	pq is the public RSA modulus, and phi(N) at must be coprime to the totient. The priva
C For data encrypti and the public keep	on or certificate verification, you will only need to y e.	he public RSA parameters: the modulus N
rime number entry		
Prime number p	251	Generate prime numbers.
Prime number q	269	
RSA parameters		
RSA modulus N	67519	(public)
phi(N) = (p-1)(q-1)	67000	(secret)
Public keye	65537	
Private key d	2473	Update parameters
SA encryption using	e / decryption using d	
Input as 🛈 text	C numbers	Alphabet and number system gptions
	_	
Input text		
RUBY FALLS!		
Input text RUBY FALLS! The Input text will be	separated into segments of Size 1 (the symbol	"#" is used as separator).
Input text RUBY FALLSI The Input text will be R # U # B # Y # #	separated into segments of Size 1 (the symbol F#A#L#L#S#!	"#" is used as separator).
Input text RUBY FALLSI The Input text will be R # U # B # Y # # Numbers input in bas	separated into segments of Size 1 (the symbol F#A #L#L#S #! e 10 format.	# is used as separator).
Input text RUBY FALLSI The Input text will be R # U # B # Y # # Numbers input in bas 082 # 085 # 066 # I	separated into segments of Size 1 (the symbol ' F # A # L # L # S # ! e 10 format. 189 # 032 # 070 # 065 # 076 # 076 # 083 # 0.	₩ is used as separator). 33
Input text RUBY FALLSI The Input text will be R # U # B #Y # # Numbers input in bas 082 # 085 # 066 # I Encryption into ciphe	separated into segments of Size 1 (the symbol F # A # L # L # S # ! e 10 format. 89 # 032 H 070 # 065 # 076 # 076 # 083 # 0 rtext c[i] = m[i] <sup>*</sup> e (mod N)	W is used as separator).
Input text RUBY FALLSI The Input text will be R # U # B # Y # # Numbers input in bes 082 # 085 # 066 # I Encryption into ciphe 58455 # 30900 # 02	separated into segments of Size 1 (the symbol F # A # L # L # S # I to 10 format. 189 # 032 # 070 # 065 # 076 # 076 # 083 # 0 read cj] = m(j] ° (mod N) 593 # 37260 # 28032 # 04562 # 16634 # 365	14" is used as separator) 33 569 # 36569 # 39103 # 03240

The number "#" serves here to visually split up the individual numbers. If you insert these numbers into the input line and then choose Decrypt, the original plaintext will be restored.

4. Click Alphabet and number system optionsChoose All 256 ASCII characters under Alphabet options, b-adic under Method for coding and a block into numbers and 2 in Block length in characters.

Alphabet options	s
All 256 ASC All 256 ASC	CII characters
C Specify alp	habet: Number of characters: 256
ABCDEFG	HIJKLMNOPQRSTUVWXYZ
RSA variant	
	C Dialogue of the <u>Sisters</u>
dethod for codir	ng a block into numbers
b-adjc	C Number system
Block length	
The number of The maximum s number of char	characters that are encrypted with each RSA operation. size of a block is limited by the bit length of the modulus N, the racters in the alphabet, and the encoding method.
Block length in	characters: 2 (Maximum block length 2 characters)
Number system-	
The numbers following radix:	or encryption and decryption will be represented in the
G. During	C Binary C Octal C Hexadecimal
• <u>D</u> ecimai	
ve Decimai	

5. To confirm your entries, click on OK.

C 0	and public key or using only the public k	ey
(p-1)(q-1) is the E key d is then calc	<ul> <li>numbers p and q. The composite number uler totient. The public key e is freely chose ulated such that d = e<sup>^</sup>(-1) (mod phi(N)).</li> </ul>	N = pq is the public HSA modulus, and phi[N] = en but must be coprime to the totient. The privat
<ul> <li>For data encryption</li> <li>and the public ket</li> </ul>	on or certificate verification, you will only ne y e.	ed the public RSA parameters: the modulus N
rime number entry		
Prime number p	251	Generate prime numbers
Prime number q	269	
RSA parameters		
RSA modulus N	67519	(public)
phi(N) = (p-1)(q-1)	67000	(secret)
Public keye	65537	
Private key d	2473	Update parameters
Private key d	2473	Update parameters
Private key d ISA encryption using	2473 e / decryption using d	Update parameters
Private key d RSA encryption using Input as (© text	2473 e / decryption using d C numbers	Update parameters
Private key d RSA encryption using Input as ret text Input text	2473 e / decryption using d C numbers	Update parameters
Private key d RSA encryption using Input as (© text Input text IRUBY FALLS1	2473 e / decryption using d C numbers	Alphabet and number system gptions
Private key d ISA encryption using Input as retext Input text RUBY FALLS!	2473 e / decuption using d C numbers	Update parameters
Private key d ISA encryption using Input as (* text Input text RUBY FALLSI The Input text will be	2473 e / decuption using d f unmbers separated into segments of Size 2 (the syn	Alphabet and number system gptions
Private key d ISA encryption using Input as rext Input text RUBY FALLSI The Input text will be RU # BY # F # AL 1	2473 e / decryption using d C numbers separated into segments of Size 2 (the syn #LS #1	Alphabet and number system gptions
Private key d BSA encryption using Input as (* text Input text RUBY FALLSI The Input text will be RU # BY # F # AL I Numbers input in bas		Lipdate parameters
Private key d RSA encryption using Input as retext Input text RUBY FALLSI The Input text will be RU # BY # F # AL Numbers input in bas 21/172 # 15995 # 06	2473  e / decuption using d  c numbers  separated into segments of Size 2 (the syn #LS # 1  e 10 formet.  p 21 1577 & # 19579 # 19490	Lipdate parameters
Private key d RSA encryption using Input as • text Input text [RUBY FALLS] The Input text will be [RU # BY # F # AL 1: Numbers input in bas [21077 # 16985 # 06	2473           e / decuption using d           C           numbers           separated into segments of Size 2 (the syn           #LS #1           = 10 format.           262 # 16716 # 19539 # 08480	Lipdate parameters
Private key d ISA encryption using Input as  text Input text RUBY FALLSI The Input text will be RU # BY # F # AL I Numbers input in bas 21077 # 16385 # 06 Encryption into ciphe		Lipdate parameters
Private key d ISA encryption using Input as  text Input text RUBY FALLSI The Input text will be RU # BY # F # AL t Numbers input in bas 21077 # 16985 # 06 Encryption into ciphe 63813 # 17874 # 31	2473 e / decyption using d f uncertained into segments of Size 2 (the syn t LS H I t LS H I t LS G Uncertained into segments of Size 2 (the syn t LS H I t LS G Uncertained into segments of Size 2 (the syn t LS H I) t LS G Uncertained into segments of Size 2 (the syn t LS H I) t LS H I t LS	Lipdate parameters
Private key d SA encryption using Input as  text Input text RUBY FALLSI The Input text will be RU # BY # F # AL I Numbers input in bas 21077 # 16985 # 00 Encryption into ciphe 63813 # 17874 # 31	2473 e / decsption using d mumbers separated into segments of Size 2 (the sym # LS # 1 = 10 format. 262 # 16716 # 19539 # 08480 rtext c[i] = m(i) <sup>Te</sup> (mod N) 769 # 54458 # 53353 # 60216	Lipdate parameters

6. You will receive a cipher text that is only half as long:

#### Cryptool: Attack on RSA encryption with short RSA modulus

The analysis is performed in two stages: first of all the prime factorization of the RSA modulus is calculated using factorization, and then in the second

stage the secret key for encryption of the message is determined. After this, the cipher text can be decrypted with the cracked secret key.

We will figure out plaintext given RSA modulus n = 63978486879527143858831415041 Public exponent e = 17579 Cipher text = 45411667895024938209259253423, 16597091621432020076311552201, 46468979279750354732637631044, 32870167545903741339819671379

1. Factorization of the RSA modulus with the aid of prime factorization.

To break down the natural number, select menu sequence Indiv. Procedure/RSA Cryptosystem / Factorization of a Number.



2. The two components of the public key is

RSA modulus n = 63978486879527143858831415041

Public exponent e = 17579

Enter n=63978486879527143858831415041 as input and click Continue.

Alexaldaria for fortalization	land
Algorithms for factorization          Image: Algorithms for factorization         Image: Brute-force         Image: Brent         Image: Pollard         Image: Pollard         Image: Williams         Image: Lenstra         Image: Quadratic sieve         Flactorization (stepwise)         Click: "Costinue" to factor the input "to factor the input"to factor the input"to factor the in	Enter the number to be factorized:
the button again to execute the fact	forization.
<u>Continue</u> Factorization The factorization is represented in the Composite numbers are highlighted	ne format <z1^a1 *="" z2^a2="" zn^an="">. in red.</z1^a1>
Factorization The factorization is represented in the Composite numbers are highlighted Last factorization through: Pollard Factorization result:	ne format <z1^a1 *="" z2^a2="" zn^an="">. in red. Found 2 factors in 0.261 seconds.</z1^a1>
Eontinue         Factorization         The factorization is represented in the Composite numbers are highlighted         Last factorization through:         Pollard         Factorization result:         145295143558111 * 44033465477            Details	ne format <z1^a1 *="" z2^a2="" zn^an="">. in red. Found 2 factors in 0.261 seconds. 7631</z1^a1>

It is interesting to see which procedure broke down the RSA modulus the fastest.

2. Calculate the secret key d from the prime factorization of n and the public key e:

With the knowledge of the prime factors p = 145295143558111 and q = 440334654777631 and the public key e = 17579, we are in a position to decrypt the ciphertext.

3. Open the next dialog box via menu selection Indiv.

Procedure/RSA Cryptosystem/RSA Demonstration:.

4. Enter p = 145295143558111 and q = 440334654777631 and the public key e = 17579.

5.Click on Alphabet and number system options and make the following settings:

Alphabet options: Specify alphabet

RSA variant: Normal

Method for coding a block into number: Number system

## Block length: 14 Number system: Decimal

Alphabet options All 256 <u>A</u> SCII Specify alpha	characters bet:	Number of chara	cters: 27
ABCDEFGHI	JKLMNOPQRSTUV	WXYZ	
RSA variant			
	C Dialogue o	f the <u>S</u> isters	
Method for coding	a block into number:	s	
⊂ b-adjc	Number system	stem	
Block length			
The number of ch The maximum size number of charac	haracters that are en e of a block is limited sters in the alphabet,	crypted with each R I by the bit length of and the encoding r	SA operation. the modulus N, the nethod.
Block length in cl	naracters: 14	(Maximum block len	gth 14 characters)
Number system			
The numbers for following radix:	encryption and decr	yption will be represe	ented in the
	C <u>B</u> inary	⊂ <u>O</u> ctal	C <u>H</u> exadecimal

5. Enter the following cipher text in the input text field. And click Decrypt button.

45411667895024938209259253423,

16597091621432020076311552201,

46468979279750354732637631044,

32870167545903741339819671379

Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) [n-1]q-1] is the Euler totient. The public key e is freely chosen but must be coprime to the totient. The private key d is then calculated such that d = e^(r-1) [mod phi(N)]. For data encryption or certificate verification, you will only need the public RSA parameters: the modulus N and the public key e. Prime number entry Prime number p [145295143558111 Generate prime numbers Prime number q [440334654777631 Generate prime numbers RSA parameters RSA modulus N [63978486879527143858831415041 (public) phi(N) = (p-1)[q-1) [63978486879526558229033079300 (secret) Public key e [17579 Private key d [10663687727232084624328285019 Lipdate parameters Ciphertext coded in numbers of base 10 [7091621432020076311552201 # 46468979279750354732637631044 # 328701675459037413398196713 Decryption into plaintext m(i) = c(j) <sup>2</sup> d (mod N) [00000000000000001401202118011200 # 0000000000001421130205181900 # 000000000000118050013 Output text from the decryption (into segments of size 14; the symbol '#' is used as separator). NATURAL NUMBERS ARE MADE BY GOD		and public key or using only the public key	
C       For data encryption or certificate verification, you will only need the public RSA parameters: the modulus N and the public key e.         Prime number entry       It45295143558111       Generate prime numbers         Prime number q       It45295143558111       (public)         Prime number q       It463978496879527143858831415041       (public)         phi(N) = (p-1)(q-1)       63978496879526558229033079300       (secret)         Public key e       I7579       Lipdate parameters         Private key d       I0663687727232084624328285019       Lipdate parameters         RSA encryption using e / decryption using d       Input as C text I rumbers of base 10       Input as C text I rumbers of base 10         [7091621432020076311552201 # 46468979279750354732637631044 # 328701675459037413398196713       Decryption into plaintext m(i] = c(i)^d (mod N)         [00000000000001401202118011200 # 0000000000001421130205181900 # 00000000000000118050013       Output text from the decryption (into segments of size 14; the symbol '#' is used as separator).       INATURAL # NUMBERS ARE MADE # BY GOD         Plaintext       INATURAL NUMBERS ARE MADE BY GOD       Inturat a set as teparator).    <	Choose two prime (p-1)(q-1) is the Eu key d is then calculated	anumbers p and q. The composite number N = pq is uler totient. The public key e is freely chosen but mu ulated such that d = e^{-1} (mod phi(N)).	the public RSA modulus, and phi(N) = ist be coprime to the totient. The privat
Prime number entry Prime number p 145295143558111 Generate prime numbers Prime number q 440334654777631 Generate prime numbers RSA parameters RSA modulus N 63978486879527143858831415041 (public) phi(N) = (p-1)(q-1) 63978486879526558229033079300 (secret) Public key e 17579 Private key d 10663687727232084624328285019 Lipdate parameters RSA encryption using e / decryption using d Input as C text I numbers Ciphertext coded in numbers of base 10 7091621432020076311552201 # 46468979279750354732637631044 # 328701675459037413398196713 Decryption into plaintext m[i] = c[i]^d (mod N) 0000000000001401202118011200 # 000000000001421130205181900 # 000000000000118050013 Output text from the decryption (into segments of size 14; the symbol '#' is used as separator). NATURAL # NUMBERS # ARE MADE # BY GOD	C For data encryption and the public key	on or certificate verification, you will only need the pu y e.	ublic RSA parameters: the modulus N
Prime number p       145295143558111       Generate prime numbers         Prime number q       440334654777631       Generate prime numbers         RSA parameters       RSA modulus N       63978486879527143858831415041       (public)         phi(N) = (p-1)(q-1)       63978486879526558229033079300       (secret)         Public key e       17579       Update parameters         RSA encryption using e / decryption using d       Input as       C text       numbers         Ciphertext coded in numbers of base 10       100000000001401202118011200 # 000000000001421130205181900 # 00000000000118050013         Decryption into plaintext m[i] = c[i]^d (mod N)       10000000000001401202118011200 # 0000000000001421130205181900 # 000000000000118050013         Output text from the decryption (into segments of size 14; the symbol '#' is used as separator).       NATURAL # NUMBERS # ARE MADE # BY GOD         Plaintext       NATURAL NUMBERS ARE MADE BY GOD       Plaintext	<sup>o</sup> rime number entry —		
Prime number q         440334654777631           RSA parameters         RSA modulus N         63978486879527143858831415041         (public)           phi(N) = (p-1)(q-1)         63978486879526558229033079300         (secret)           Public key e         17579	Prime number p	145295143558111	Generate prime numbers
RSA parameters       FSA modulus N       63978486879527143858831415041       (public)         phi(N) = (p-1)(q-1)       63978486879526558229033073300       (secret)         Public key e       17579	Prime number q	440334654777631	
RSA modulus N       63978486879527143858831415041       (public)         phi(N) = (p-1)(q-1)       63978486879526558229033079300       (secret)         Public key e       17579	RSA parameters		
phi(N) = (p-1)(q-1)       63978486879526558229033079300       (secret)         Public key e       17579       Update parameters         Private key d       10663687727232084624328285019       Update parameters         RSA encryption using e / decryption using d       Alphabet and number system options         Ciphertext coded in numbers of base 10       7091621432020076311552201 # 46468979279750354732637631044 # 328701675459037413398196713         Decryption into plaintext m(i) = c(i)^d (mod N)       0000000000001401202118011200 # 00000000001421130205181900 # 00000000000118050013         Output text from the decryption (into segments of size 14; the symbol '#' is used as separator).       NATURAL # NUMBERS # ARE MADE # BY GOD         Plaintext       NATURAL NUMBERS ARE MADE BY GOD       NATURAL NUMBERS ARE MADE BY GOD	RSA modulus N	63978486879527143858831415041	(public)
Public key e       17579         Private key d       10663687727232084624328285019       Update parameters         RSA encryption using e / decryption using d       Input as C text I rumbers       Alphabet and number system options         Ciphertext coded in numbers of base 10       7091621432020076311552201 # 46468979279750354732637631044 # 328701675459037413398196713         Decryption into plaintext m[i] = c[j]^d (mod N)       1000000000001401202118011200 # 000000000001421130205181900 # 000000000000118050013         Output text from the decryption (into segments of size 14; the symbol '#' is used as separator).       INATURAL # NUMBERS # ARE MADE # BY GOD         Plaintext       NATURAL NUMBERS ARE MADE BY GOD	phi(N) = (p-1)(q-1)	63978486879526558229033079300	(secret)
Private key d       10663687727232084624328285019       Update parameters         RSA encryption using e / decryption using d       Alphabet and number system options         Input as C text (* numbers       Alphabet and number system options         Ciphertext coded in numbers of base 10       7091621432020076311552201 # 46468979279750354732637631044 # 328701675459037413398196713         Decryption into plaintext m[i] = c[i]^d (mod N)       000000000001401202118011200 # 00000000001421130205181900 # 000000000000118050013         Output text from the decryption (into segments of size 14; the symbol '#' is used as separator).       NATURAL # NUMBERS # ARE MADE # BY GOD         Plaintext       NATURAL NUMBERS ARE MADE BY GOD	Public key e	17579	_
RSA encryption using e / decryption using d Input as C text ( numbers Liphertext coded in numbers of base 10 [7091621432020076311552201 # 46468979279750354732637631044 # 328701675459037413398196713 Decryption into plaintext m[i] = c[j]^d (mod N) [000000000001401202118011200 # 000000000001421130205181900 # 000000000000118050013 Dutput text from the decryption (into segments of size 14; the symbol '#' is used as separator). [NATURAL # NUMBERS # ARE MADE # BY GOD Plaintext [NATURAL NUMBERS ARE MADE BY GOD]	Private keu d	10663687727232084624328285019	<u>Update parameters</u>
Decryption into plaintext m[i] = c[i]^d (mod N)           [0000000000001401202118011200 # 0000000000001421130205181900 # 000000000000118050013           Output text from the decryption (into segments of size 14; the symbol '#' is used as separator).           NATURAL # NUMBERS # ARE MADE # BY GOD           Plaintext           NATURAL NUMBERS ARE MADE BY GOD	RSA encryption using	e / decryption using d	
000000000001401202118011200 # 0000000000001421130205181900 # 000000000000118050013         Output text from the decryption (into segments of size 14; the symbol '#' is used as separator).         NATURAL # NUMBERS # ARE MADE # BY GOD         Plaintext         NATURAL NUMBERS ARE MADE BY GOD	RSA encryption using Input as C text Ciphertext coded in n	e / decryption using d r numbers umbers of base 10 311552201 # 46468979279750354732637631044	habet and number system <u>o</u> ptions # 32870167545903741339819671375
Output text from the decryption (into segments of size 14; the symbol '#' is used as separator).          NATURAL #       NUMBERS #       ARE MADE #       BY GOD         Plaintext	RSA encryption using Input as C text Ciphertext coded in n 7091621432020076 Decryption into plaint	e / decryption using d (* numbers	habet and number system <u>o</u> ptions # 32870167545903741339819671375
NATURAL # NUMBERS # ARE MADE # BY GOD Plaintext NATURAL NUMBERS ARE MADE BY GOD	RSA encryption using Input as C text Ciphertext coded in n 7091621432020076 Decryption into plaint 0000000000000140	e / decryption using d	habet and number system options # 3287016754590374133981967137 1900 # 000000000000001180500130
NATURAL NUMBERS ARE MADE BY GOD	RSA encryption using Input as C text Ciphertext coded in n 7091621432020076 Decryption into plaint 0000000000000140 Output text from the c	e / decryption using d r numbers umbers of base 10 311552201 # 46468979279750354732637631044 ext m[i] = c[i]^d (mod N) 1202118011200 # 0000000000001421130205181 lecryption (into segments of size 14; the symbol '#' is	habet and number system options # 32870167545903741339819671379 1900 # 0000000000000001180500130 used as separator).
	RSA encryption using Input as C text Ciphertext coded in n 7091621432020076 Decryption into plaint 0000000000000140 Output text from the c NATURAL #	e / decryption using d	habet and number system options # 32870167545903741339819671379 1900 # 0000000000000001180500130 : used as separator).
	RSA encryption using Input as C text Ciphertext coded in n 7091621432020076 Decryption into plaint 0000000000000140 Output text from the c NATURAL # Plaintext NATURAL N	e / decryption using d r numbers umbers of base 10 311552201 # 46468979279750354732637631044 ext m[i] = c[i]^d (mod N) 1202118011200 # 0000000000001421130205181 decryption (into segments of size 14; the symbol '#' is NUMBERS # ARE MADE # BY GOD UMBERS ARE MADE BY GOD	habet and number system options # 32870167545903741339819671379 1900 # 0000000000000001180500130 s used as separator).

Check your results: "NATURAL NUMBERS ARE MADE BY GOD"

### Side Channel Attack to RSA:

Select from menu: "Analysis" \"Asymmetric Encryption" \"Side-Channel Attack on Textbook RSA"



#### Click "Introduction to the scenario".

e-Channel Attack on the Hybrid End	cryption Protocol (Textbook RSA)		X
Step-by-step attack Introduction into the scenario	Alice [Client]		Bob [Server]
Perform preparations			
Transmit message			1
Decrypt message			
Intercept message		Trudy (Attacker)	
Start attack cycle		1	
Generate report		Attack progress:	
Quit			Show information dialogs

Click "Perform preparation" and click "OK"



Click "OK" again.

Hybrid cryptosystem see https://en.wikipedia.org/wiki/Hybrid\_cryptosystem



Click "Generate session key" and "Session Key". The generated session key is e.g. "9E B7 61 D9 E4 F9 34 AA 91 F7 C4 CB 56 7D 98 88". You may obtain different key!



### Click "Select asymmetr. key".

Last name	First name	Key type	Key identifier	Created	Internal ID no.
ideChannelA	t Bob	RSA-512	PIN=1234	06.07.2006 05:51:34	1152179494
imith Imith	John Maru	RSA-1024 RSA-304	Smith Key Manukeu	12.07.2011 17:09:15 13.07 2011 09:54:04	1310504955 1310565244
ote: Here only	names are displa	ayed, which have	an RSA key.		120 3.

Select Bob's key and click "OK".



Click "Encrypt document symmetry.", "Encrypt session key asymmetry." and "Save".



Click "Transmit message" and "Decrypt message".







Click "Intercept message" and "Start attack cycle".



Click "All steps at once" button.

Side-Channel Attack Successful			
Congratulations!			
You have executed a complete side-channel attack against the hybrid encryption protocol.			
Please click on Trudy's info button to make sure whether the protocol attack really helped Trudy to decrypt the hybrid encrypted message.			
<u> </u>			

Click "OK" and icon of Trudy (Attacker).

arrent Status of Trudy	х
Action log: • Trudy has intercepted the message Alice sent to Bob • Trudy has isolated the encrypted session key from the message • Trudy has created 130 modified session keys up to now • 66 of 130 modified messages were successfully decrypted by Bob's server	
Modified and encrypted session keys:	LUD
Modified and encrupted session key (hexadecimal):	
98 35826D 01F0C1B 2867861E 6436A8B 9C0B0E 1FD 4CB 9EE 37E 6FA3B 93501A8C2D 0943E 5AE C90C854A 1698EA1 3A32A64B 44A5117B 05C8E 58E 5F81 4BB 8B CAFFAC56BA7333B 811B 9787C533B 0 6E B 2D E ACD B 24D 1 35D 2D 3A96B F675D B1 EFFB 11D B1 031 C88CAF47C0C04AB 32C3B 0 FA3E 231B 9309B 8C306B 9E 3A 1839CF465B F57992E 9386B 89E C2E 2CCE FB 1 650FAEE 83015B 93B 92268C4B 1 C4C7FC479FCA017522C 079260D B4B 7C6356E1 69207FE D 5C776506575369A6D 307641 6A806E7194B D AC98D 9335D 1 B C340A11	-
Decrypted session key (calculated by Trudy, based on Bob's responses):	
9EB761D9E4F934AA91F7C4CB567D9888	-
' Message (calculated by Trudy using the decrypted session key):	
CrypTool (Starting example for the CrypTool version family 1.x)	
CrypTool is a comprehensive free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.	
	-
ΩK	

The session key is 9EB761D9E4F934AA91F7C4CB567D9888 which matches the one generated in Step 5.