Assignment6

Lab on Short Message RSA Attacks and Padding (100 points)

In **short message attack of RSA**, if it is known that Alice is sending a four-digit number to Bob, Eve can easily try plaintext numbers from 0000 to 9999 to find the plaintext. Therefore, short message must be padded with random bits. **If you are Eve, show that you are able to find the plaintext containing four digit numbers given ciphertext.**

Optimal asymmetric encryption padding (OAEP) is recommended when short messages are encrypted with RSA algorithms. The following is the encryption and decryption processes of OAEP.

- Encryption
 - Pad the message to make m-bit message M, if M is less than m-bit
 - Choose a random number r
 - User one-way function G that inputs r-bit integer and outputs m-bit integer. This is the mask.
 - P1 = M ⊕ G[®]
 - P2 = H(P1) ⊕ r, function H inputs m-bit and outputs k-bit
 - C = E(P1 || P2). User RSA encryption here
- Decryption
 - P = D (P1 || P2)
 - Bob first recreates the value of r:
 - $\mathsf{H}(\mathsf{P1}) \oplus \mathsf{P2} = \mathsf{H}(\mathsf{P1}) \oplus \mathsf{H}(\mathsf{P1}) \oplus \mathsf{r} = \mathsf{r}$
 - Bob recreates msg:
 - $G(r) \oplus P1 = G(r) \oplus G(r) \oplus M = M$

Pad your message with OAEP padding and then encrypt by RSA.

What to submit:

A report describes how you find the unpadded short plaintext (30 points), describes what you have observed after you apply OAEP padding (30 points), and discusses feasibility of short message attack after padding (10 points).

Lab on RSA Encryption and Factorization Attacks (practice)

Encryption or decryption of messages using the RSA key pair.

1. Select Individual Procedures/RSA Cryptosystem/RSA Demonstration

👷 CrypTool 1.4.30 - startingexample-en.txt				
File Edit View Encrypt/Decrypt Digital Signatures/PKI	Indiv. Procedures Analysis Options Window Help			
□☞■■● メ ▣ € ♂ … ? ?	Hash			
	RSA Cryptosystem Prime Number Test			
Yr startingexample-en.txt	Protocols Generate Prime Numbers			
CrypTool (Starting example for the CrypTool version far	Chinese Remainder Theorem Applications			
CrypTool is a comprehensive free educational program	Visualization of Algorithms RSA Demonstration			
offering extensive online help and many visualizations.	Secret Sharing Demonstration (Shamir) Signature Demonstration (Signature Generation)			
This is a text file, created in order to help you to make	Tools			
 As a first step it is recommended you read the inclu of the online help can be accessed via the menu "Help online help. Press F1 to start the online help everywhere in CryoTon 	Educational Games Number Theory - Interactive available functions within this application. The starting page the search keyword "Starting page" within the index of the available functions within this application. The starting page the search keyword "Starting page" within the index of the available functions within this application. The starting page the search keyword "Starting page" within the index of the available functions within this application. The starting page the search keyword "Starting page" within the index of the available functions within this application. The starting page the search keyword "Starting page" within the index of the available functions within this application. The starting page the search keyword "Starting page" within the index of the available functions within this application. The starting page the search keyword "Starting page" within the index of the available functions within the available functions within the index of the available functions wit			
 A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (Classic)". There are several examples (tutorials) provided within the online help which provide an easy way to gain an understanding of cryptology. These examples can be found 				
Via the menu "Help -> Scenarios (Tutorials)". 4) You can also develop your knowledge by: - Navigating through the menus. You can press F1 at any selected menu item to get further information. - Reading the included Readme file (see the menu "Help -> Readme"). - Viewing the included colorful presentation (This presentation can be found on several ways: e.g. in the "Help" menu of this application, or via the "Documentation" section - Viewing the webpage www.cryptool.org.				

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.

	and public key or using only the public key	I
Choose two prime (p-1)(q-1) is the Ei key d is then calc	e numbers p and q. The composite number N uler totient. The public key e is freely chosen ulated such that d = e^(-1) (mod phi(N)).	= pq is the public RSA modulus, and phi(N) = but must be coprime to the totient. The priva
 For data encryptic and the public ke 	on or certificate verification, you will only need y e.	d the public RSA parameters: the modulus N
^p rime 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
3SA encruption using	e / decryption using d	
torn on organismus	Г	,
Input as 📀 text	C numbers	Alphabet and number system options
Input as • text Enter the message fo	C numbers r encryption or decryption either as text or as	Alphabet and number system options
Input as • text Enter the message fo	C numbers r encryption or decryption either as text or as	Alphabet and number system options
Input as retext Enter the message fo	C numbers (r encryption or decryption either as text or as	Alphabet and number system options
Input as text	C numbers	Alphabet and number system options
Input as (* text	C numbers r encryption or decryption either as text or as	Alphabet and number system options
Input as (* text	C numbers r encryption or decryption either as text or as	Alphabet and number system options
Input as retext	C numbers r encryption or decryption either as text or as	Alphabet and number system options
Input as retext	C numbers r encryption or decryption either as text or as	Alphabet and number system options

3. Click Alphabet and number system options

RSA Demonstration Options	x
Alphabet options All 256 ASCII characters Specify alphabet: All 256 ASCII characters: 256	
RSA variant	
• Normal • 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:	
● <u>D</u> ecimal ○ <u>B</u> inary ○ <u>O</u> ctal ○ <u>H</u> exadecim	nal
	el

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

RSA Demonstration Options	
Alphabet options C All 256 ASCII characters Image: Specify alphabet: Number of characters: 27 ABCDEFGHIJKLMNOPQRSTUVWXYZ	
RSA variant Image: Second state of the se	
Method for coding a block into numbers O b-adjc • Number system	
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: 2 (Maximum block length 2 characters)	
Number system The numbers for encryption and decryption will be represented in the following radix: • Decimal • Decimal • Binary • Decimal • Hexadecimal • Output	
<u>D</u> K	

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.

RSA Demonstration		— X—	
 RSA using the private and public key or using only the public key Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = (p-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⁽⁻¹⁾ (mod phi(N)). 			
 For data encryption and the public key e 	or certificate verification, you will only nee ».	d 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	
⊢RSA encryption using e /	decryption using d		
Inputas 🕫 text 📿) numbers	Alphabet and number system options	
Input text			
WORKSHOP AT CHAT	WORKSHOP AT CHATTANOOGA		
The Input text will be se	parated into segments of Size 2 (the symb	ool '#' is used as separator).	
WO # RK # SH # OP #	‡ A # T # CH # AT # TA # NO # OG #.	A	
Numbers input in base 10 format.			
2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100			
Encryption into ciphertext c[i] = m[i]^e (mod N)			
1999 # 3408 # 2545 #	2798 # 0001 # 3284 # 3613 # 1404 # 2	932 # 0208 # 1095 # 3306	
Encrypt	Decrypt	Close	

6. To decrypt, copy text in <u>Encryption into ciphertext</u> **1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 #** 3306 to <u>input text</u> area. And click **Decrypt** button.

RSA using the private and public key or using only the public key Image: Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi[N] = [p-1](a-1) is the Euler totient. The public key e is freely chosen but must be coprime to the totient. The private key dist then calculated such that d = e^{-(1)} [mod phi[N]). Image: Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi[N] = [p-1](a-1) is the Euler totient. The private key dist then calculated such that d = e^{-(1)} [mod phi[N]). Image: Choose two prime number p image: Choosen but must be coprime to the totient. The private key dist then calculated such that d = e^{-(1)} [mod phi[N]). Prime number entry Prime number q Prime number q [79 RSA parameters Generate prime numbers Prime number q [79 RSA modulus N [3713 phi[N] = (p-1](q-1) [3588 (secret) [public key e Public key e [37 Private key d [97 RSA encryption using e / decryption using d [phi[N] = (p-1](q-1) Input as C text (• numbers Alphabet and number system options Ciphertext coded in numbers of base 10 [1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 Decryption into plaintext m[i] = c[i] ² d (mod N) [2315 # 1811 # 1908 # 1516	A Demonstration			— ×
Image: Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = [p-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^(-1) (mod phi(N)). Image: Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = [p-1](q-1) is the calculated such that d = e^(-1) (mod phi(N)). Image: Choose two prime number p is the public RSA parameters: the modulus N and the public key e. Prime number p is prime number p is the public RSA parameters. RSA parameters RSA modulus N is prime number g is prime number subtrime numbers Prime number q is prime number g is prime number g is the public key e is freely choosen but must be coprime numbers Prime number q is prime number g is	- RSA using the private 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 Prime number entry 47 Prime number p 47 Generate prime number q 73 RSA parameters Generate prime numbers Psime number q 73 RSA parameters Generate prime numbers Psime number q 73 RSA modulus N 3713 phi(N) = (p-1)(q-1) 3588 Public key e 37 Private key d 97 Explorate to the compton using e / decryption using d Imput as C text (● numbers Input as C text ● numbers Ciphertext coded in numbers of base 10 1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 Decryption into plaintext m[i] = c[i]^2 (mod N) 2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100 Output text from the decryption (into segments of size 2; the symbol '#' is used as separator). WO # RK # SH # OP # A # T # CH # AT # TA # NO # 0G # A Plaintext WORKSHOP AT CHATTANOGA Close	Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = [p-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^[-1] (mod phi(N)).			
Prime number entry Prime number p 47 Prime number p 47 Generate prime numbers Prime number q 79 Generate prime numbers RSA parameters RSA modulus N 3713 (public) phi(N) = (p-1)(q-1) 3568 (secret) Public key e 37 Update parameters RSA encryption using e / decryption using d Input as C text I numbers of base 10 Ipage 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 Decryption into plaintext m[i] = c[i]^d (mod N) [2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100 Output text from the decryption (into segments of size 2; the symbol "#' is used as separator). [WO # RK # SH # OP # A # T # CH # AT # TA # NO # 0G # A Plaintext [WORKSHOP AT CHATTANOOGA Close	 For data encryption and the public key 	n or certificate verification, you will on e.	nly need the public RSA (parameters: the modulus N
Prime number p 47 Generate prime numbers Prime number q 79 Generate prime numbers RSA parameters RSA modulus N 3713 (public) phi(N) = (p-1)(q-1) 3588 (secret) Public key e 37 Update parameters Private key d 97 Update parameters RSA encryption using e / decryption using d Input as Alphabet and number system gptions Ciphertext coded in numbers of base 10 1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 Decryption into plaintext m[i] = c[i]^d (mod N) 2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100 Output text from the decryption (into segments of size 2; the symbol ## is used as separator). [W0 # RK # SH # 0P # A # T # CH # AT # TA # N0 # 0G # A Plaintext	Prime number entry			
Prime number q 79 RSA parameters RSA modulus N 3713 (public) phi(N) = (p-1)(q-1) 3588 (secret) Public key e 37	Prime number p	47		Generate prime numbers
RSA parameters Image: State of the st	Prime number q	79		
RSA modulus N 3713 (public) phi(N) = (p-1)(q-1) 3588 (secret) Public key e 37	RSA parameters			
phi(N) = (p-1)(q-1) 3588 (secret) Public key e 37 Update parameters Private key d 97 Update parameters RSA encryption using e / decryption using d Alphabet and number system options Input as C text I numbers Input as C text I numbers of base 10 1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 Decryption into plaintext m[i] = c[i]^d (mod N) [2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100 Output text from the decryption (into segments of size 2; the symbol '#' is used as separator). WO # RK # SH # OP # A # T # CH # AT # TA # NO # 0G # A Plaintext WORKSHOP AT CHATTANOOGA Close	RSA modulus N	3713		(public)
Public key e 37 Private key d 97 Input as O text I numbers Alphabet and number system options Ciphertext coded in numbers of base 10 1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 Decryption into plaintext m[i] = c[i]^d (mod N) 2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100 Output text from the decryption (into segments of size 2; the symbol '#' is used as separator). WO # RK # SH # OP # A # T # CH # AT # TA # NO # 0G # A Plaintext WORKSHOP AT CHATTANOOGA Close	phi(N) = (p-1)(q-1)	3588		(secret)
Private key d 97 Update parameters RSA encryption using e / decryption using d Alphabet and number system options Input as C text I Input as C text Information numbers of base 10 Alphabet and number system options Ciphertext coded in numbers of base 10 1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 Decryption into plaintext m[i] = c[i]^d (mod N) 2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100 Output text from the decryption (into segments of size 2; the symbol '#' is used as separator). WO # RK # SH # OP # A # T # CH # AT # TA # NO # 0G # A Plaintext WORKSHOP AT CHATTANOOGA Close	Public key e	37		
RSA encryption using e / decryption using d Input as C text Imput as Alphabet and number system options Ciphertext coded in numbers of base 10 Imput as 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 Decryption into plaintext m[i] = c[i]^d (mod N) Imput as 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100 Output text from the decryption (into segments of size 2; the symbol '#' is used as separator). Imput work # SH # OP # A # T # CH # AT # TA # NO # OG # A Plaintext Imput work # SH # OP # A # T # CH # AT # TA # NO # OG # A Encrypt Decrypt	Private key d	97		Update parameters
Input as C text • numbers Ciphertext coded in numbers of base 10 []999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 [] Decryption into plaintext m[i] = c[i]^d (mod N) [] <td>-RSA encryption using e</td> <td>/ decryption using d</td> <td></td> <td></td>	-RSA encryption using e	/ decryption using d		
Ciphertext coded in numbers of base 10 1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 Decryption into plaintext m[i] = c[i]^d (mod N) 2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100 Output text from the decryption (into segments of size 2; the symbol '#' is used as separator). W0 # RK # SH # 0P # A # T # CH # AT # TA # NO # 0G # A Plaintext W0RKSH0P AT CHATTANOOGA	Inputas 🔿 text	• numbers	Alphabet and	number system <u>o</u> ptions
Image: Second state in the second s	Ciphertext coded in nu	mbers of base 10		
Decryption into plaintext m[i] = c[i]^d (mod N) 2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100 Output text from the decryption (into segments of size 2; the symbol '#' is used as separator). W0 # RK # SH # OP # A # T # CH # AT # TA # NO # OG # A Plaintext W0RKSHOP AT CHATTANOOGA	1999 # 3408 # 2545	# 2798 # 0001 # 3284 # 3613 # 140	04 # 2932 # 0208 # 109	5 # 3306
2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100 Output text from the decryption (into segments of size 2; the symbol '#' is used as separator). W0 # RK # SH # OP # A # T # CH # AT # TA # NO # OG # A Plaintext W0RKSHOP AT CHATTANOOGA	, Decruption into plainte	xt m[i] = c[i]^d (mod N)		
Output text from the decryption (into segments of size 2; the symbol '#' is used as separator). W0 # RK # SH # OP # A # T # CH # AT # TA # NO # OG # A Plaintext W0RKSHOP AT CHATTANOOGA Encrypt Decrypt	2315 # 1811 # 1908	# 1516 # 0001 # 2000 # 0308 # 012	20 # 2001 # 1415 # 150	7 # 0100
W0 # RK # SH # OP # A # T # CH # AT # TA # NO # OG # A Plaintext W0RKSHOP AT CHATTANOOGA	Output text from the dr	ecruption (into segments of size 2: the	e sumbol '#' is used as se	parator)
Plaintext WORKSHOP AT CHATTANOOGA Encrypt Close				
Encrupt Close				
		TTANOOCA		
Encrypt Close	WURKSHUP AT CHA	ATTANUUGA		
	Encrypt	Decrypt		Close

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. The value of N is ______, the value of phi(N) is ______, the value of private key d is ______.

sse using the private.	and public key or using only the public key	
 Choose two prime (p-1)[q-1] is the Eikey d is then calc 	enumbers p and q. The composite number N ler totient. The public key e is freely chosen ulated such that d = e^(-1) (mod phi(N)).	= pq is the public RSA modulus, and phi(N) = but must be coprime to the totient. The privat
 For data encryption and the public ket 	on or certificate verification, you will only need y e.	I the public RSA parameters: the modulus N
rime number entry-		
Prime number p	251	Generate prime numbers
Prime number q	269	
SA parameters		
RSA modulus N	67519	(public)
phi(N) = (p-1)(q-1)	67000	(secret)
Public key e	65537	
Private key d	2473	Update parameters
	e / decryption using d	
SA encryption using		
SA encryption using	C numbers	Alphabet and number system options
ISA encryption using Input as r (• <u>text</u> Enter the message fo	numbers	Alphabet and number system options
RSA encryption using Input as • text Enter the message fo	numbers	Alphabet and number system <u>o</u> ptions hex dump.
ISA encryption using Input as	C numbers	Alphabet and number system options hex dump.
RSA encryption using Input as	numbers	Alphabet and number system <u>o</u> ptions hex dump.
ISA encryption using Input as	numbers	Alphabet and number system <u>o</u> ptions hex dump.
ISA encryption using Input as	numbers	Alphabet and number system <u>o</u> ptions hex dump.
ISA encryption using	numbers	Alphabet and number system <u>o</u> ptions hex dump.
Input as	C numbers	Alphabet and number system <u>o</u> ptions hex dump.

2. Click Alphabet and number system options

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

RSA Demonstration Options
Alphabet options • All 256 ASCII characters • Specify alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
RSA variant Image: Second state s
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 2 characters)
Number system The numbers for encryption and decryption will be represented in the following radix: • Decimal • Binary • Decimal • Hexadecimal
<u>D</u> K <u>C</u> ancel

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.

RSA Demonstration		×		
 RSA using the private and public key or using only the public key Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = (p-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 = e¹(-1) (mod phi(N)). 				
C For data encryptio and the public key	Provide a second sec			
Prime 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 a	e / decryption using d			
Input as 🔎 text	C numbers	Alphabet and number system options		
Input text				
RUBY FALLS!				
The Input text will be :	separated into segments of Size 1 (the syr	nbol '#' is used as separator).		
R#U#B#Y# #F	F#A#L#L#S#!			
Numbers input in base	, Numbers input in base 10 format.			
082 # 085 # 066 # 0	082 # 085 # 066 # 089 # 032 # 070 # 065 # 076 # 076 # 083 # 033			
Encruption into cicheri	, Ensuration into sinkertout ofil – mill^s (mod N)			
58455 # 30900 # 02	58455 # 30900 # 02593 # 37260 # 28092 # 04562 # 16634 # 36959 # 36959 # 39103 # 03240			
Encrypt	Decrypt	Close		

The encrypted version of this is the number sequence is ______

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 options

Choose **All 256 ASCII characters** under <u>Alphabet options</u>, **b-adic** under <u>Method for coding and a block</u> <u>into numbers</u> and **2** in <u>Block length in characters</u>.

RSA Demonstration Options	×
Alphabet options All 256 ASCII characters Specify alphabet: ABCDEFGHIJKLMN0PQRSTUVWXYZ	acters: 256
BSA variant © <u>N</u> ormal © Dialogue of the <u>S</u> isters	
Method for coding a block into numbers O b-adjc Number system	
Block length The number of characters that are encrypted with each F The maximum size of a block is limited by the bit length of number of characters in the alphabet, and the encoding r Block length in characters: 2 (Maximum block length)	RSA operation. the modulus N, the method. ngth 2 characters)
Number system The numbers for encryption and decryption will be repression following radix: Image: Comparison of the decryption of the decryption will be repression of the decryption of the decryption will be repression of the decryption	ented in the C <u>H</u> exadecimal
	<u>C</u> ancel

5. To confirm your entries, click on **OK**.

RSA Demonstration		×		
RSA using the private and public key or using only the public key				
Choose two prime n (p-1)[q-1) is the Eule key d is then calcula	Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = (p-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 ⁽⁻¹⁾ (mod phi(N)).			
 For data encryption and the public key e 	 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	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			
Input as 💿 text	numbers	Alphabet and number system options		
Input text				
RUBY FALLS!				
The Input text will be se	parated into segments of Size 2 (the syn	ubol '#' is used as separator).		
RU # BY # F # AL # L	S #!			
Numbers input in base 10 format.				
21077 # 16985 # 08262 # 16716 # 19539 # 08480				
Encryption into cipherte	Encryption into ciphertext c[i] = m[i]^e (mod N)			
63813 # 17874 # 31769 # 54458 # 53353 # 60216				
Encrypt	<u>D</u> ecrypt	<u>C</u> lose		

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

Attack on RSA encryption with short RSA modulus (practice)

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.

🥰 CrypTool 1.4.30		Roberts Inc. Manual Red
File Edit View Encrypt/Decrypt Digital Signature	s/PKI Indiv. Procedures Analysis Options Window Help	2
	Hash >	
	RSA Cryptosystem	Prime Number Test
	Protocols •	Generate Prime Numbers
	Chinese Remainder Theorem Applications	Factorization of a Number
	Visualization of Algorithms	RSA Demonstration
	Secret Sharing Demonstration (Shamir)	Signature Demonstration (Signature Generation)
	Tools	Lattice Based Attacks on RSA
	Educational Games	
	Number Theory - Interactive	
	Number I neory - Interactive	

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.

Factorization of a Number	
Algorithms for factorization	_ Input
Brute-force	
🔽 Brent	Enter the number to be factorized:
✓ Pollard	63978486879527143858831415041
Villiams	
🔽 Lenstra	
Quadratic sieve	
Factorization (stepwise) Click "Continue" to factor the input number. the button again to execute the factorization	If the result (shown below) can be factored further, click n.
Factorization The factorization is represented in the forma Composite numbers are highlighted in red. Last factorization through: Pollard Factorization result:	at <z1^a1 *="" z2^a2="" zn^an="">. Found 2 factors in 0.261 seconds.</z1^a1>
145295143558111 * 440334654777631	4
<u>D</u> etails	
	Close

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

RSA Demonstration Options
Alphabet options C All 256 <u>A</u> SCII characters Number of characters: 27 Specify alphabet: ABCDEEGHUKI MNOPORSTUNAXXZ
RSA variant • <u>N</u> ormal • <u>N</u> ormal
Method for coding a block into numbers O b-adjc • Number system
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: 14 (Maximum block length 14 characters)
Number system The numbers for encryption and decryption will be represented in the following radix:
● <u>D</u> ecimal ○ <u>B</u> inary ○ <u>O</u> ctal ○ <u>H</u> exadecimal
<u>OK</u> <u>Cancel</u>

6. Enter the following cipher text in <u>the input text</u> field. And click **Decrypt** button.

45411667895024938209259253423, 16597091621432020076311552201, 46468979279750354732637631044, 32870167545903741339819671379

RSA Demonstration		×	
RSA using the private and public key or using only the public key			
(• Choose two prime numbers p and q. The composite number N = pq is the public HSA modulus, and phi(N) = (p-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 ⁽⁻¹⁾ (mod phi(N)).			
C For data encryption and the public key	or certificate verification, you will only need the publice.	c RSA parameters: the modulus N	
Prime number entry			
Prime number p	145295143558111	Generate prime numbers	
Prime number q	440334654777631		
- RSA parameters			
RSA modulus N	63978486879527143858831415041	(public)	
phi(N) = (p-1)(q-1)	63978486879526558229033079300	(secret)	
Public keye	17579		
Private key d	10663687727232084624328285019		
RSA encryption using e	/ decryption using d		
Input as O text I numbers Alphabet and number system options			
Ciphertext coded in nu	mbers of base 10		
70916214320200763	1552201 # 46468979279750354732637631044 # 3	2870167545903741339819671379	
Decryption into plainte:	κt m[i] = c[i]^d (mod Ν)		
0000000000001401202118011200 # 000000000001421130205181900 # 00000000000011805001301			
Output text from the de	cryption (into segments of size 14; the symbol '#' is us	ed as separator).	
NATURAL #	NUMBERS # ARE MADE # BY GOD		
Plaintext			
NATURAL NU	MBERS ARE MADE BY GOD		
Encrypt	Decrypt	Close	

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

Side Channel Attack to RSA: (10 points)

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

Step-by-step attack	Alice [Client]		Bob [Server]
Introduction into the scenario			
Perform preparations			
Transmit message			
Decrypt message			
		- Trudu (Attacker)	
Start attack cycle		i	
Generate report		Attack progress:	
Quit			Show information dialogs

2. Click "Introduction to the scenario".

Step-by-step attack	Alice [Client]		Bob [Server]
Introduction into the scenario			
Perform preparations			
Transmit message	_		†
Decrypt message			
Intercept message		- Trudu féttackad	
Start attack cycle			
Generate report		Attack progress:	
			Show information dialogs

3. Click "Perform preparation" and click "OK"



4. Click "OK" again.



5. Click "Generate session key" and "Session Key". The generated session key is "9E B7 61 D9 E4 F9 34 AA 91 F7 C4 CB 56 7D 98 88".



6. Click "Select asymmetr. key".

RSA key for the hy	brid encryptic	on	•		×
Select the receive	er key from the l	list.			
Last name	First name	Key type	Key identifier	Created	Internal ID no.
SideChannelAt	Bob	RSA-512	PIN=1234	06.07.2006 05:51:34	1152179494
Smith	John	RSA-1024	Smith Key	12.07.2011 17:09:15	1310504955
Smith	Mary	RSA-304	Mary key	13.07.2011 09:54:04	1310565244
1					
Note: Here only na	ames are display	yed, which have a	an RSA key.		
OK					Cancel
	_				

7. Select Bob's key and click "OK".



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



9. Click "Transmit message" and "Decrypt message".



10. Enter 1234 and click "OK".

Side-Channel Attack on the Hybrid Encry	ption Protocol (Textbook RSA)		x
Step-by-step attack Introduction into the scenario Perform preparations	Alice [Client]		Bob [Server]
Transmit message			
Decrypt message Intercept			
Start attack cycle Generate report		Trudy [Attacker]	
Quit			Show information dialogs

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



12. 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> ОК]

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

Current Status of Trudy
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
Intercepted, encrypted session key:
A1D9E964CE3862AB029389C16C3B384E78A89B0E28CE62B63026156E0A1ACD3FF833DABEBEDD6EA8E0B
Modified and encrypted session keys:
Modified and encrypted session key (hexadecimal):
9B35826D01F0C1B2867861E6436A8B9C0B0E1FD4CB9EE37E6FA3B93501A8C2D0943E5AEC90C854A
B24D135D2D3A96BF675DB1EFFB11DB1031C88CAF47C0C04AB32C3B0FA3E231B9309B8C306B9E3A 1839CF465BF57992E9386B89EC2E2CCEFB1650FAEE83015B93B92268C4B1C4C7FC479FCA017522C 079260DB4B7C6356E169207FFD5C776506575369A6D3076416A806F7194BDAC98D9335D1BC340A11
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.
<u><u> </u></u>

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