

**Ministry of Education, Culture and Research of the Republic of Moldova**

**Technical University of Moldova**

**Department of Software and Automation Engineering**

**REPORT**

Laboratory Work Nr.6

Discipline: Cryptographic methods of information protection

Realised by: st.gr. FAF-213 Iațco Sorin

Checked by : asist.univ.   
 Mîțu Cătălin

Chișinău 2023

**Subject:** Hash functions and digital signatures

# **Tasks:**

**Task 2.** Using the wolframalpha.com platform or the Wolfram app Mathematica, generate keys, perform signing and digital signature validation a to the message m that you obtained by completing laboratory work no. 2. The signing will be done by applying the RSA signature. The value of n must be of at least 3072 bits. The hash algorithm will be selected from the list below accordingly with the formula i = (k mod 24) +1, where k is the student's order number in the list group, i is the index of the hash function in the list:

1. MD4 2. MD5 3. MD2 4. MD6-128 5. MD6-256 6. MD6-512 7. SHA-1 8. SHA-224 9. SHA-256 10. SHA-384 11. SHA-512 12. SHA3-224 13. SHA3-256 14. SHA3-384 15. SHA3-512 16. RipeMD-128 17. RipeMD-160 18. RipeMD-256 19. RipeMD-320 20. Whirlpool 21. NTLM 22. Haval192,3 23. Haval224,4 24. Haval256,4

**Task 3.** Using the wolframalpha.com platform or the Wolfram app Mathematica, perform signing and digital signature validation of message m onwhich you obtained by completing laboratory work no. 2. The signature will be achieved by applying the ElGamal signature (p and generator are given lower). The hash algorithm will be selected from the list below according to formula i = (k mod 24) +1, where k is the student's order number in the list group, i is the index of the hash function in the list:

1. NTLM 2. MD4 3. MD5 4. MD2 5. MD6-128 6. MD6-256 7. MD6-512 8. SHA-1 9. SHA-224 10. SHA-256 11. SHA-384 12. SHA-512 13. SHA3-224 14. SHA3-256 15. SHA3-384 16. SHA3-512 17. RipeMD-128 18. RipeMD-160 19. RipeMD-256 20. RipeMD-320 21. Whirlpool 22. Haval192,3 23. Haval224,4 24. Haval256,4

Note:

For tasks 2 and 3 use the decimal numerical representation of a the message, reaching it through the hexadecimal representation of the characters, in according to ASCII encoding. For convenience in conversion you can use the page https://www.rapidtables.com/convert/number/hex-to decimal.html.

For task 3 considered

p=3231700607131100730015351347782516336248805713348907517458843413926

980683413621000279205636264016468545855635793533081692882902308057347

262527355474246124574102620252791657297286270630032526342821314576693

141422365422094111134862999165747826803423055308634905063555771221918

789033272956969612974385624174123623722519734640269185579776797682301

462539793305801522685873076119753243646747585546071504389684494036613

049769781285429595865959756705128385213278446852292550456827287911372

009893187395914337417583782600027803497319855206060753323412260325468

4088120031105907484281003994966956119696956248629032338072839127039,

which has 2048 bits and the generator g=2.

**Hash algorithm:**

Haval192,3

# **RSA signature:**

First of all I hash the message using *Haval192,3* algorithm, from the tool online, then this message digest is sent to the RSA encryption algorithm.

For the RSA algorithm firstly I generated 2 primes, *p1* of 464 digits and another *p2* of 463 digits using WolframAlpha, so that *n* has 3090 bits. Next the *n* is computed by multiplying *p1* and *p2*, next is computed by the formula. The *e* value is chosen from a random interval from 1 to -1, the *e* value is checked if it’s valid and is saved. Next the *d* value is calculated by formula .

The encryption process is straight forward, . The decryption as follows, .

After encryption, the plain text message and the digital signature are sent to be decrypted. The receiver uses the same hash algorithm that was used for encryption to create his own message digest. Using the public key received to decrypt the digital signature using RSA algorithm decryption process, the result being the original message digest (hash). The last step is comparing if the obtained hash is equal to the initial hash of the sender.

# **RSA Results:**

***m*** =

yardley's appropriation had been severely cut in 1924, and half thestaff had to be let go,  
reducing the force to about a dozen. despite this,yardley said, the black chamber managed to  
solve, from 1917 to 1929,more than 45,000 telegrams, involving the codes of argentina,  
brazil,chile, china, costa rica, cuba, england, france, germany, japan,liberia, mexico, nicaragua,  
panama, peru, san salvador, santo domingo(later the dominican republic) the soviet union, and  
spain and madepreliminary analyses of many other codes, including those of the vatican.suddenly  
it all ended. yardley, who had been obtaining the codetelegrams of foreign governments through  
the cooperation of thepresidents of the western union telegraph company and the  
postaltelegraph company, was encountering increasing resistance from them.herbert hoover had  
just been inaugurated, and yardley resolved to settle the matter with the new  
administration once and for all. hedecided on the bold stroke of drawing up "a memorandum to  
bepresented directly to the president, outlining the history and activities ofthe black  
chamber, and the necessary steps that must be taken if thegovernment had hoped to take full  
advantage of the skill of itscryptographers." he waited to see which way the wind was blowing  
beforemaking his move—and found that it was not with him. yardley went to aspeakeasy to listen  
to hoover's first speech as president and sensed, inthe high ethical strictures that  
hoover expressed, the doom of the blackchamber.he was right, though its actual closing came  
from elsewhere. afterhenry l. stimson, hoover's secretary of state, had been in office the  
fewmonths that yardley thought would be necessary for him to have lostsome of his innocence  
in wrestling with the hardheaded realities ofdiplomacy, the black chamber sent him the  
solution of an importantseries of messages. but stimson was different from previous  
secretariesof state, on whom this tactic had always worked. he was shocked tolearn of the  
existence of the black chamber, and totally disapproved of it.he regarded it as a low, snooping  
activity, a sneaking, spying, keyhole-peering kind of dirty business, a violation of the  
principle of mutual trustupon which he conducted both his personal affairs and his  
foreignpolicy. all of this it is, and stimson rejected the view that such meansjustified  
even patriotic ends. he held to the conviction that his countryshould do what is right,  
and, as he said later, "gentlemen do not readeach other's mail." in an act of pure moral courage,  
stimson, affirmingprinciple over expediency, withdrew all state department funds from  
thesupport of the black chamber.\* since these constituted its majorincome, their loss  
shuttered the office. hoover's speech had warnedyardley that an appeal would be fruitless.  
there was nothing to do butclose up shop.in 1940, as secretary of war, he had to reverse  
himself and acceptthe cryptanalyses of magic. but the international situation then  
wastotally different. "in 1929," he himself has written, in the third person,"the world was  
striving with good will for lasting peace, and in this effortall the nations were parties.  
stimson, as secretary of state, was dealingas a gentleman with the gentlemen sent as ambassadors  
and ministersfrom friendly nations. ..." in 1940, europe was at war, and the unitedstates was  
on the verge.the signal corps, where william friedman had charge of cryptology.the staff quickly  
dispersed (none went to the army), and when the bookswere closed on october 31, 1929, the  
american black chamber hadperished. it had cost the state department $230,404 and the  
wardepartment $98,808.49—just under a third of a million dollars for adecade of cryptanalyis.  
yardley, whose job experience had been rather specialized, could notfind work, and he went back  
home to worthington. the depressionsucked him dry. by august of 1930, he had had to give up  
an apartmenthouse and a one-eighth interest in a real estate corporation; indeed,  
hecomplained that he had to sell nearly everything he owned "for less thannothing." a few  
months later he was toying with the idea of writing thestory of the black chamber to make some  
money to feed his wife andtheir son, jack. when his old mi-8 friend, manly, with whom he hadbeen  
in contact all during the 1920's, had to turn down his request for a$2,500 loan at the end of  
january, 1931, yardley, in desperation, satdown to write what was to be the most famous book on  
cryptology everpublished.

***mHash*** = cfd7f6906d8765cbcceb9471b8673edc78f6cbd27f3ae07e

***n*** =

18176345774690490145005943209717669474131091104775151597497993608485278105507909626588461987910412858390632857180349285985785079487932129763913739914001378106999348755681627984347072790259781207539457644917982657508360532436539450130732192019158928885610714988479720173969821017960607077788944850999948213389505915699564825694632532422589390921072521380565974753621292457451717635675531473354950051514033163893610848375495717760124576904775195076811727042720229082394472877539134362184259336776222918322310418962366635255789180111949126114181331839401346560426990988696992961524314098057862720986941907962524166911660385561846528716062541653499866837602762241860812259367567607534366708139640270890057055245795529151806306702386966156514075367963936254956368749022365558655144767417517613300523303944851933695461262096435248209432820018181148533926136688843433177114619470025800486805886919831661897820325221973824876972877383

n: 926 digits 3090 bits

=

18176345774690490145005943209717669474131091104775151597497993608485278105507909626588461987910412858390632857180349285985785079487932129763913739914001378106999348755681627984347072790259781207539457644917982657508360532436539450130732192019158928885610714988479720173969821017960607077788944850999948213389505915699564825694632532422589390921072521380565974753621292457451717635675531473354950051514033163893610848375495717760124576904775195076811727042720229063669109854921231018818754750133545811569946761481214288849524886449851943767290372287801339019601606007087083397183219362340820537397945397017092081066734701272407133869310471958073633443729981460340391591436509262539909749383847844871531107117643180041977108998386310253654089200590431687758351757737858819230523979883245110451975028858832705960505051489439053666798755737983574926498343352937821699563565869428151148674742485575435253172086310464841904508744760

***digital signature*** =

15104073870210956359147030730487067477320887032214930163125337435093126877012067381436656227868040706164900369425129433092963106829603807519142501433912812790732469700821563140275608377106418011389987225667088428759966070614474498252993569677339611997122404604176545629557642240728741461324982315558798529796883742849939058589436020986752380509290183012427679946830365546729534242734291413272643757626974478844258002385882572773199361065712699903231200560429759057522592836829028291076434513729833745653116405246344476066215570768841660363861512798161046133289709841758581571552162517230049779517107248425842380371020903189511307471140576749740855693959768160034924848265149145714607690120733899729023244957315100502654318293638133009024422189814302184889962235121527572939797672103194421936089862602324561920531333217959517129824749758537266246609297466083026863658298106175651039616432936789216157462067129947180701341860980

# **ElGamal signature:**

The signing process is as follows, first of all choosing a prime *k*, calculate *r* so r = g^k mod p, next calculate *h* = hash(M), where hash is the hashed message using *Haval192,3* algorithm. After that calculate *s* = (h — xr) \* k^-1 mod (p-1). The digital signature sent to the receiver is the pair (*r, s*).

Verification is done in the next steps, using the public key, first calculate the hash for the received plain text message using the same hash algorithm as the sender, then calculate *v1* = (y^r \* r^s) mod p, next calculate *v2* = g^h mod p. Finally if *v1* and *v2* are equal the signature is valid, if not is invalid.

The hash and the decimal equivalent remains the same from RSA, because the methods for generation are the same.

# **ElGamal Results:**

***k*** = 79

***y =***

974016807176741595973807437573386333506424047430680977969913110822645570945445877802957602763663100938960096450147514671869964184955311579878378540181366914567989685897853392166142860403609469328988420898444228030520790441044361000606003848213809877176676809014201459168862711930650022361283916912186920415550178128164874984649553943719942626798573294155780190573029813444528734474640188359593356842023850530836411672918224140576202658661409365085633611000564728654524973974034860664731253887798131577717557569791637581163338766443198329369760939686338620600399539979295676899268703338879982200384949228333939374385

***r =*** 604462909807314587353088

***s =***

23292565763806915783146408543891238439260427374482501149662235099391508265456578023835903143979715670775627322595745031520820888521780368204743078086133226759410855198645006879156869264841714803136327818125810188656854152918272307057057300905906318455644253880198264285303627523166585946796600910196011353436240756040799966569230556657384706294416900519560015482633219552998514558220404627167269760329244120186877374663376696048610210540057891818747749922078949023127678872426488182035716552787998577290399792351386760021868980115769435491528726778664971456350021979751031525718914920894425196222315528453443175339686

***v1*** =

23896275292215199093985069647127010046118952799527921623074150574504360735539862712007404622884646759400318575763341217551171348287266542232498408502270807653067209554392216994312469590474835193083305382512684361557856662728182863655719204103383519747385987909608108834724272717920245351897228506364059878112941536790753714040072942450287745297968761925450253326816861902028979996340332453155199184728650233927006406243018222475377634925793944971528559096403366783525179833529621681830516705225636621346185423063344579782501203017612531434895168127891460507031097242475873605645548827459701387870587451231698773399861

***v2*** = ***v1***

# **Conclusion:**

In conclusion, this laboratory work not only provided a hands-on experience with the implementation of RSA and ElGamal digital signatures but also fostered a deeper appreciation for the principles that underpin modern cryptographic protocols and hash algorithms. The exploration of these widely used algorithms enhances my understanding of secure communication methods and prepares me to address the ongoing challenges and advancements in the field of cryptography.

# **Resources:**

[CS-Labs/lab6 at main · Syn4z/CS-Labs (github.com)](https://github.com/Syn4z/CS-Labs/tree/main/lab6)