

RLING

The Cryptographic Technique Using Python for Secure Transfer of Data

Jeffery Gardner Jr

Yenumula B Reddy (Advisor)

LAS 2016, Alexandria, LA, USA - April 23, 2016

Louisiana Academy of Sciences - April 23, 2016





- Background
- RSA Algorithm
- RSA Encryption and Decryption
- Message in operation Encryption and Decryption



Background

Number of threats increased in terms of Laptops or storage devices; Therefore, people started storing information in cloud based environment and process;

It became a requirement to

Support safe cloud applications using encrypted algorithms

Create encrypted Apps so that information transferring is safe from source

Provide safe storage and retrieval of information with minimum cost without compromising Quality of service





The understanding of problem background is:

Previously, information security was	Today it is about "confidentiality
mainly about "keeping a secret"	
Breaking secret code is part of	Encryption and decryption is part of secret
understanding the secret	today
Person or system behind that	Identity of someone or something is the
information	information we want to authenticate
Internet is not centrally managed	Therefore, security became important for
and much responsibility is pushed	survival; Security is deployed at node and
node level; Most of the users are	network level; The wildest solution is
does not understand much of	cryptographic;
computer or security	



Environment

The tools and techniques that were used to execute this operation were:

- Server/Client model
- RSA Algorithm
- TCP communication
- MD5 cryptographic hash function
- Command Line





Client/Server Model







Cryptographic Hash Functions (Objective)

- Authentication
- Message Integrity
- Message Fingerprinting
- Error Detection
- Digital Signature Efficiency





Original Message

story.txt

The following is a large collection of stories and anecdotes about clueless computer users. It's a baffling phenomenon that in today's society an individual, who might in other circumstances be considered smart and wise, can sit down in front of a computer screen and instantly lose every last shred of common sense he ever possessed. Complicate this phenomenon with a case of "computerphobia," and you end up with tech support personnel having phone conversations that are funny in retrospect but seem like perfectly valid motives for wild machine gun shooting sprees at the time. And yet, amidst the vast, surging quantities of stupidity are perfectly excusable technological mishaps -- but that are amusing nonetheless. After all, even the best of us engages in a little brainless folly every once in a while. Most of these stories are true. Some happened to me personally. Some happened to friends of mine. Some are considered urban legends, but even most of these are more likely to have happened in some form or another than not. Skeptics look at such stories and doubt their truth. But reason, common sense, and experience tell me that if you sit someone who isn't computer literate (even a smart someone) down in front of a computer, you're bound to accrue anecdotes no less outrageous than these. You'd be surprised.

>>>
Please enter the filname that you wish to open
story
1a4e2ca520ca09f5e179e5f15906e8b1
>>>



GRAMBLING

Altered Message

story.txt*

The following is a large collection of stories and anecdotes about clueless computer users. It's a baffling phenomenon that in today's society an individual, who might in other circumstances be considered smart and wise, can sit down in front of a computer screen and instantly lose every last shred of common sense he ever possessed. Complicate this phenomenon with a case of "computerphobia," and you end up with tech support personnel having phone conversations that are funny in retrospect but seem like perfectly valid motives for wild machine gun shooting sprees at the time. And yet, amidst the vast, surging quantities of stupidity are perfectly excusable technological mishaps -- but that are amusing nonetheless. After all, even the best of us engages in a little brainless folly every once in a while. Most of these stories are true. Some happened to me personally. Some happened to friends of mine. Some are considered urban legends, but even most of these are more likely to have happened in some form or another than not. Skeptics look at such stories and doubt their truth. But reason, common sense, and experience tell me that if you sit someone who isn't computer literate (even a smart someone) down in front of a computer, you're bound to accrue anecdotes no less outrageous than these. You'd be surprised

>>>

Please enter the filname that you wish to open story 235224727f44f9e4cc137cdae783380b >>>



GRAMBLING STATE UNIVERSITY

Cryptographic Hashing

WHERE EVERYBODY IS SOMEBODY





STATE UNIVERSITY

Message For Simulation

story.txt

The following is a large collection of stories and anecdotes about clueless computer users. It's a baffling phenomenon that in today's society an individual, who might in other circumstances be considered smart and wise, can sit down in front of a computer screen and instantly lose every last shred of common sense he ever possessed. Complicate this phenomenon with a case of "computerphobia," and you end up with tech support personnel having phone conversations that are funny in retrospect but seem like perfectly valid motives for wild machine gun shooting sprees at the time. And yet, amidst the vast, surging guantities of stupidity are perfectly excusable technological mishaps -- but that are amusing nonetheless. After all, even the best of us engages in a little brainless folly every once in a while. Most of these stories are true. Some happened to me personally. Some happened to friends of mine. Some are considered urban legends, but even most of these are more likely to have happened in some form or another than not. Skeptics look at such stories and doubt their truth. But reason, common sense, and experience tell me that if you sit someone who isn't computer literate (even a smart someone) down in front of a computer, you're bound to accrue anecdotes no less outrageous than these. You'd be surprised.











RSA Encryption

WHERE EVERYBODY IS SOMEBODY

```
Got connection from ('10.70.28.55', 51950)
Now encrypting message and creating the MD5 Digest ...
Encrypting and writing to message.txt...
Encrypted text:
1337 128 145373019385333978715847868509023251835343676731086551311806123520878008
276035439185128870404039715239470546358455125102363799624813089918436576669311056
302492450183861146839886912112753538956466825863401305267745824960974667463615865
597722602292713848473987617932861533510796092983387762715038708979794651650649019
793620777970127980088716873978128539029943598068995933600012051011806118602730914
933425601138348845119351977504733082240563158656292648070407494886291777515354139
950029990714731655259353144950593780590191273317947731131222078882550227988138051
62446630069795925872356916021116104563746731812564468485682,751490743627935219921
284219418772511169623647086519282009415212783111692542735815034477700975666907548
123964040093964191711418552810619776881817807650143889135573445799489358623345841
503185179648775994683805592612598076950643192115932341779386437290283451324171132
827447885463893795236869407408452672776843926810641248164635860376658131733020955
654536294618745418923384587112671832609512202008555117074091217088581111660323456
479229145932024200680906960239527898641100207220107374754865267684677110412692602
866296940661441478128419538723366982907173511791894021728590210861767090716159947
5307865562705269456320821790,5238480738593847550020462799966121068348079528569515
107188039994610838067107894600049392030721835634890610166667495519093998799086844
618187666686741751722869735280589740486304628301073511144543779258208236838014776
543015353665985807505340763417420806983756174229995817387340518698222748323611732
137042991986744737685562498660201839305198057200502604271208018699677933018098229
167352715766571719787076569692403880602563343508324652006946662095937591664433716
351316339945992522906362455216240436938394400159659578093838371696882887765677591
218714413000631777468523549468332290159398124163827408082742101573176646475841,17
951775094568539790761509343469193408174716912793892550172429685335706923307480478
646307190186624991608039771109549871882394666825250453984448412582768235345584512
282706436888333970823236091158109324812847621611498737946504019329117010834825949
038871598408892222632999321875872711408998363702380424232861301529613466645672457
679654968126264945392604047989250981095905262413165790530025523088162151064796545
697775377051107500969513842253805399733769062022919304179240768529463394878365897
```

New thread started for 10.70.28.55: 51950





File Transfer

file opened
receiving data
file close()
Successfully got the file
connection closed
clock: start = 5.862066741974684e-07 end = 2.3253669800332144
clock: duration_clock = 2.32536639382654
time: start = 1459394297.554934 end = 1459394299.88018
time: duration time = 2.3252458572387695





Decryption Operation

Reading from encrypted_file.txt and decrypting...

Decrypted text:

The following is a large collection of stories and anecdotes about clueless computer users. It's a baffling phenomenon that in today's society an individual, who might in other circumstances be considered smart and wise, can sit down in front of a computer screen and instantly lose every last shred of common sense he ever possessed. Complicate this phenomenon with a case of "computerphobia," and you end up with tech support personnel having phone conversations that are funny in retrospect but seem like perfectly valid motives for wild machine gun shooting sprees at the time. And yet, amidst the vast, surging quantities of stupidity are perfectly excusable technological mishaps -- but that are amusing nonetheless. After all, even the best of us engages in a little brainless folly every once in a while. Most of these stories are true. Some happened to me personally. Some happened to friends of mine. Some are considered urban legends, but even most of these are more likely to have happened in some form or another than not. Skeptics look at such stories and doubt their truth. But reason, common sense, and experience tell me that if you sit someone who isn't computer literate (even a smart someone) down in front of a computer, you're bound to accrue anecdotes no less outrageous than these. You'd be surprised.

2/9/2017







