

Welcome, Hacke3erDD. Control Panel Inbox Alerts (0) Logout

Myanmar Security Forum

[HOME](#)[MEMBERS](#)[HELP DOCS](#)[UPGRADE](#)[AWARDS](#)[BLACKLIST](#)[GROUPS](#)

Myanmar Security Forum - MSF >
Hacking > Cryptography > Digging into RSA Algorithm

[TODAY'S POSTS](#)[NEW POSTS](#)

Thread Rating: ★★★★★

[New Reply](#)

Digging into RSA Algorithm

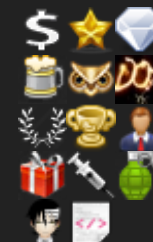
[Thread Modes](#)

Luna

Administrator



Posts: 958
Threads: 0
Thanks
Received: 429
in 188 posts
Thanks Given:
241
Joined: Oct
2013
Reputation:
119



03-28-2016, 01:39 PM


#1

Digging into RSA Algorithm


အစကဘယ်လိုရေးရမှန်းမသိဘူးကိုဖြစ်နေတာ နောက်တော့လည်း ရှိသမျှဟာတွေလိုက်ဖတ် ကောင်းတဲ့ရှင်းထားတာလေးတွေမှတ်ထားကနေ ခုတော့ ရေးလို့တောင်ပြီးသွားပါပြီ။ နည်းနည်းတော့ရှုပ်မယ်။ ဒါပေမယ့်လို့ သေချာဖတ်ရင်တော့ နားလည်သွားမှာပါ။ နားမလည်ဘူးဆိုလည်း ဝင်ဆွေးနွေးသွားနိုင်ပါတယ်။ မှားနေတာတစ်ခုခုကိုတွေ့တယ်ဆိုရင်လည်း အားမနာနဲ့ ဝင်ပြောသွားပါ။ မဟုတ်က ဟုတ်ကကြီးရေးထားမိရင် သာ ရှက်ရပါလိမ့်မယ် 😊

What is RSA ?

RSA ဆိုတာ public-key ကိုအသုံးပြုတဲ့ Cryptosystem ဖြစ်ပါတယ်။ Crypto တွေကိုဘယ်နေရာမှာသုံးတာလဲဆိုတာတော့ တွေ့တွေထူးထူးပြောနေဖို့လိုတော့မယ်မထင်ပါဘူး။ ဆက်လေ့လာမယ်။ RSA ကို ၁၉၇၇ ခုနှစ်မှာ Ron Rivest , Adi Shamir , Leonard Adleman တို့က စတင်ဖော်ပြခဲ့ခြင်းဖြစ်ပါတယ်။ သူတို့၃ ယောက်နာမည်တွေကိုအစွဲပြုပြီးတော့ RSA (Rivest-Shamir-Adleman) ဆိုပြီးဖြစ် လာခဲ့တယ်။ Public Key Cryptography လို့ခေါ်တယ်နောက်တစ်ခုက Asymmetric cryptography လို့လည်းခေါ်ပါတယ်။ ဒီနေရာမှာ Assymmetric cryptography အကြောင်းပြောဖို့လိုလာပြီ။ အရင်လေ့လာခဲ့တဲ့ cryptography တွေအကုန်လုံးက symmetric key ခေ တွဖြစ်ပါတယ်။ ဘာကွားခြားမှုရှိသလဲဆိုရင် အရင် cryptography တွေမှာ key ကတစ်ခုတည်းပဲ။ Encrypt လုပ်လည်း ဒီ Key ပဲ Decrypt လုပ် မယ်ဆိုလည်းဒီ key ပဲ။ ဒါကိုမြန်မာလိုဆိုရင်တော့ ခေါက်ချိုးညီတယ်ပေါ့။ ဟုတ်ပြီ Asymmetric မှာတော့ ဒီလိုမဟုတ်တော့ဘူး ။ Encrypt လုပ်ဖို့ကို Key တစ်ခု Decrypt လုပ်ဖို့ကို Key တစ်ခု။ Encrypt ကို Public-Key နဲ့လုပ်တယ်ဆို Decrypt လုပ်တဲ့အခါတော့ private-key ကို သုံးမှရမယ်။ ဒီလောက်နားလည်ထားရင်ရပါပြီ။

 [Image: rsa_encryption.jpg]

Encrypt လုပ်တဲ့ public-key ကို လူတိုင်းသိနိုင်ပေမယ့် private-key ကိုတော့ secret အနေနဲ့ထားမှဖြစ်ပါလိမ့်မယ်။ ဒါမှသာ လုံခြုံမှုရှိတော့မှာပေါ့။ Protocol တွေဖြစ်ကြတဲ့ SSH , OpenPGP , S/MIME , SSL/TLS စတာတွေမှာလည်း RSA ကို Encryption အတွက်ရယ် Digital Signature အတွက်သုံးကြပါတယ်။ Digital Signature ကိုအောက်မှာပုံလေးထည့်ပေးထားပါတယ်။

 [Image: ss_digitalsignature_2014_v01_desktop.png]

RSA Operation

RSA မှာ Public Key create လုပ်ဖို့ဆိုရင် အဓိကလိုအပ်တာကတော့ Prime Number ၂ ခုပဲဖြစ်ပါတယ်။ ဒီ prime number ၂ ခုဟာ လျှို့ဝှက်ထားရမှာဖြစ်ပါတယ်။ ဒါဆိုရင် ပိုပြီးလေ့လာကြတာပေါ့။ အတတ်နိုင်ဆုံးတော့ရှင်းပြလိုက်မယ်။ နားမလည်ဘူးဆိုရင်တော့ တစ်မျိုးကြံကြံတာပေါ့။

ဟုတ်ပြီ Prime Numbers တွေပါဝင်တဲ့ ကိန်းသေ ၂ ခုရှိမယ်။ p & q ပဲဖြစ်ပါတယ်။

$n = pq$ ကတော့ RSA key ရဲ့ bit length ပဲဖြစ်ပါတယ်။ ဥပမာ 1024 bits RSA ဘာဘာညာညာပေါ့။
 ဟုတ်ပြီနော်။ Public Key မှာ modulus n နဲ့ public exponent e (ပုံမှန်အားဖြင့်တော့ 65537) တို့ပါဝင်မယ်။
 Private Key မှာကတော့ modulus n နဲ့ private exponent d တို့ပါဝင်ပါတယ်။ d တန်ဖိုးကိုတွက်တဲ့အခါမှာတော့ Euler's Totient ကိုသုံးပြီးတွက်ရမှာဖြစ်ပါတယ်။
 ဒါကို မြန်မာလိုဘယ်လိုခေါ်မလဲတော့ ဂျာနောလည်း Maths သမားမဟုတ်တော့မသိသေးဘူး။ အသိထဲမှာလည်း Maths သမားမရှိတော့မသိဘူးဖြစ်နေတယ်။ ဆောရီးပါ။ ဒါပေမယ့်လို့စိတ်မပူပါနဲ့ တွက်တဲ့အခါဂျာနားလည်အောင်ရှင်းပြပေးပါမယ်။
 ခုဆို ဖတ်နေတဲ့သူတွေတော်တော်လေးကိုရှုပ်ကုန်ပြီ။ မှတ်ပဲမှတ်ထားလိုက်ပါ။ Example လေးတွေလုပ်လိုက်ရင် နားလည်သွားမှာပါ။

A Simple , worked example

ဟုတ်ပြီ။ ဂျာနော Thin Ba Shane က RSA key တစ်ခုကို generate လုပ်မယ်ဆိုပါတော့ဗျာ။ Prime Number 2 ခုကို p & q အတွက်ရွေးချယ်လိုက်ပြီ။
 $p=11$, $q=13$ ။ ဒီတော့ modulus $n = 143$ ဖြစ်သွားပြီ။ Totient Function ကိုသုံးရမယ်။ ဒီတော့ကာ
 $\phi(n)=(p-1) \times (q-1) = (11-1) \times (13-1) = 120$ ။
 နောက်ပြီးတော့ဂျာနောတို့ public key အတွက် e တန်ဖိုးကို 7 လို့ရွေးလိုက်မယ်။ ဘာကြောင့် 7 ကိုရွေးရတာလဲဆိုတာပြောပါမယ်။ public key အတွက် e တန်ဖိုးကိုရွေးတဲ့အခါမှာ
 Greatest Common Divisor (gcd) ကို $\phi(n)$ တန်ဖိုးနဲ့ အနည်းဆုံး 1 ရှိတာကိုရွေးချယ်ဖို့လိုပါတယ်။
 3 , 5 စတဲ့ Prime Number တစ်ခုခုကိုရွေးလိုက်တယ်ဆိုရင် $\phi(n)$ တန်ဖိုးဖြစ်တဲ့ 120 နဲ့ gcd 1 မရှိဘူး။ ဒါကြောင့်ရွေးလို့မရလို့ 7 ကိုရွေးလိုက်တာဖြစ်တယ်။ ဟုတ်ပြီ။ ဒါဆိုရင် ဂျာနောတို့ e တန်ဖိုးကို 7 ကိုရပြီဆိုပါတော့။ private key အတွက် d တန်ဖိုးကို တွက်ရမယ်။ ဘယ်လိုတွက်ရမလဲဆိုတော့ 7 ရဲ့ inverse တန်ဖိုးကို $\phi(n)$ နဲ့ တွက်ရမယ်။ တွက်ရမယ့် formula က $n-1 = m \pmod{p}$ ဖြစ်တယ်။ $n = 7$, $p=120$ ဆိုပြီးတွက်ရမှာပေါ့။ ဒါပေမယ့် နားလည်ထားရင်ရပါပြီ။
 ဂျာနောကတော့

Code:

<http://www.cs.princeton.edu/~dsri/modular-inversion-answer.php?n=7&p=120>

ဟောဒီမှာသွားတွက်လိုက်တယ်ဗျာ။ Manual နားလည်တယ်ဆိုပေမယ့် အကုန်လိုက်လုပ်နေရရင်လည်းသေရချည်းရဲ့ပေါ့။
 ဂျာနောတို့ရလာတဲ့ d တန်ဖိုး 103 မှန်မမှန်ကို $e \cdot d = 1 \pmod{\phi(n)}$ ဆိုတဲ့ Formula လေးသုံးပြီးပြန်စစ်ကြည့်မယ်။ $7 \cdot 103 = 721 = 1 \pmod{120}$ အိုကေပြီ။

ဟုတ်ပြီ။ ဒါဆိုရင် 9 ဆိုတဲ့ plain text လေးနဲ့ encrypt / decrypt လုပ်ကြည့်ကြမယ်။ formula အရ 9 ဟာ m တန်ဖိုးဖြစ်တယ်ဆိုတာသိထားရပါမယ်။

Encryption (using public key $e, n = 7, 143$)

$$M_e \pmod{n} = 9^7 \pmod{143} = 48 = C$$

Decryption (using private key $d, n = 103, 143$)

$C_d \bmod n = 48_{103} \bmod 143 = 9 = M$

အောက်ကနေတဲ့ d တို့, e တို့က to the power ကိုပြောတာပါ အပေါ်တင်မရဘူးဖြစ်နေလို့. 🙄

ဒီလောက်ဆို ကုန်ော Friend တွေ RSA သဘောတရားကိုနားလည်ပြီလို့ ယူဆပါတယ်။ ကုန်ောပြောခဲ့တာလေးတွေကိုပြန်ပြီး တစ်ခုချင်းစမ်းသပ်မယ်ဆို ပိုပြီးနားလည်လာမှာသေချာတယ်။ ဒီတော့ ဘယ်လိုစမ်းမှာလဲ ခွဲတွက်စရာမလိုပါဘူး။ အောက်ကပေးထားတဲ့ Link မှာသွားတွက်ကြည့်ပါ။ တစ်ဆင့်ချင်းကိုတွက်ကြည့်လို့ရပါတယ်။

Code:

<http://logos.cs.uic.edu/340%20notes/rsa.html>

Real World Example

Real world အနေနဲ့ ကုန်ောတို့ "attack at dawn" ဆိုတဲ့ plain text ကိုစမ်းကြည့်ရမယ်။ ဟုတ်ပြီ။ ပထမဆုံးဘာစလုပ်ရမလဲဆိုတော့ ကုန်ောတို့ "attack at dawn" က Ascii format တွေဖြစ်နေတယ်မလား။ ဒါကိုအရင်ဆုံး Numeric တွေပြောင်းပြစ်ရမယ်။ ဒါမှ encrypt လုပ်လို့ရမှာနော်။ အပေါ်မှာ 9 ကိုလုပ်ပြထားတာမှတ်မိသေးပါတယ်။ string ကနေ bit array တန်ဖိုးတွေပြောင်းလိုက်မယ်ဆိုရင်တော့ Numeric တွေရပြီပေါ့။ 1976620216402300889624482718775150 ဖြစ်သွားမယ်။ အောက်မှာ Converter Link ပေးထားပါတယ်။

Code:

https://gist.github.com/barrysteyn/4184435#file_convert_text_to_decimal.py

Key Generation လုပ်ဖို့အတွက် p & q တန်ဖိုးကို Prime Number တွေ generate လုပ်ရမယ်။ ဟိုဥပမာတုန်းကလို 11 13 တွေမရတော့ဘူး။ ဒီတော့ Rabin-Miller primality tests ကိုသုံးပြီး generate လုပ်ကြမယ်။ အောက်ကဟာလေးသုံးကြည့်။ ကိုယ့်ဖာသာလည်း ကြိုက်ရာရာကြည့်လို့ရတယ်။

Code:

<http://www.javascripter.net/math/primes/millerrabinprimalitytest.htm>

p

Code:

```
1213107243921127189732367153161244042847242763370141092563454931230196437304208561932419736532241686654
1017057361365214171711713797974299334871062829803541
```

q

Code:

```
1202752425547874888595622079373451212873338780368207543365389998395517985098879789986914690080913161115
3346817050832096022160146366346391812470987105415233
```

p နဲ့ q ကိုရပြီး ဒါဆို n နဲ့ $\phi(n)$ တန်ဖိုးကိုတွက်လို့ရပြီ။

n

Code:

```
1459067680075833232301869393490706352924018723753571643995818710198734387990053589383695714026701498021
2181808629246742282815702292207674690654340122488967247240792696998710058129010319931785875366371086235
7656510507883714297115637342788911463535102712032765166518411726859837988672111837205085526346618740053
```

 $\phi(n)$ **Code:**

```
1459067680075833232301869393490706352924018723753571643995818710198734387990053589383695714026701498021
2181808629246742282815702292207674690654340122488964831381123227996631730139777785236530154784827347887
1297222058587457152891606459269718119268971163555070802643999529549644116811947516513938184296683521280
```

e - the public key

65537 ကိုသုံးရမယ် ဒါကိုပဲသုံးကြတယ်လို့အပေါ်မှာပြောခဲ့တယ်။ ပြီးတော့ gcd of 1 with $\phi(n)$ ရှိရမယ်လေ။

d - the private key

Code:

```
8948942500927444436822854592177309391966958606588425744549785445648767483962981839093494197326287961679
7970608917283679875499331574161113854088813275488110588247193077582527278437906504015680623423550067240
042466665654232383502922215493623289472138866445818789127946123407807725702626644091036502372545139713
```

Encryption

1976620216402300889624482718775150_e mod n

Code:

```
3505211133867302669021242393705332851188076081157998162064280234668581062310985023594304908097338624111
3784040794704193978215378499765413083646438784740952306932534945195080183861574225226218879827232453912
820596886440377536082465681750074417459151485407445862511023472235560823053497791518928820272257787786
```

Decryption

35052111338673026690212423937053328511880760811579981620642802346685810623109
85023594304908097338624111378404079470419397821537849976541308364643878474095
23069325349451950801838615742252262188798272324539128205968864403775360824656
81750074417459151485407445862511023472235560823053497791518928820272257787786
dmodn

Code:

1976620216402300889624482718775150 (which is our plaintext "attack at dawn")

Refrence : SearchSecurity , Wikipidea , doctrina , ucdenvr, and googling

နည်းနည်းပွင်းဖို့ ကောင်းနေလိမ့်မယ်။ နောက်တစ်ခါ ဒါနဲ့ ပတ်သတ်တဲ့ Challenge လေးတစ်ခုဖြေကြမယ်။ ဒါကိုမသိရင်တော့ Challenge ဖြေ
တဲ့အခါဂျာရင် ဟိုလိုလိုဒီလိုလိုဖြစ်နေမှာစိုးလို့ ဒါလေးအရင်ရေးပေးလိုက်တာ။
ပြီးပါပြီ။ နားလည်ကြပါစေလို့ မျှော်လင့်ပါတယ်။ 🙌

Best Regard Luna



<http://www.thinbashane.wordpress.com>



Jabber : mrx@creep.im

PM

Find

Add Thank You

Reply

Quote

Report



Hades.y2k •

Moderator



Posts: 287
Threads: 0
Thanks
Received: 65
in 31 posts
Thanks Given:
18
Joined: Feb
2014
Reputation:
103

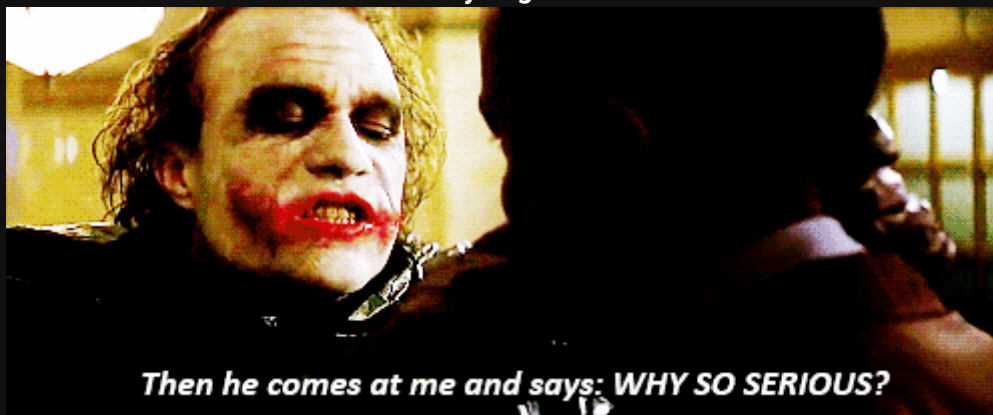


03-28-2016, 09:48 PM (This post was last modified: 03-28-2016, 09:49 PM by Hades.y2k.)

#2

အမှန်အတိုင်းဝန်ခံရရင် post ကြီးပဲဖတ်တာဘာမှနားမလည်လိုက်ဘူး ဘရိုပြောသလို link မှာသွားတွက်ကြည့်မှပဲသဘောပေါက်လာတယ်
ဒါနဲ့အခုနောက်ပိုင်း AES Encryption လဲသုံးကြတယ်ဘရို NSA က classified information တွေကို AES 256 encryption နဲ့ပို့တယ်တောင်ပြော
တယ်
သိသလောက်လေးဝင်ဆွေးနွေးကြည့်တာ 🙏

hadesy2k.github.io



PM

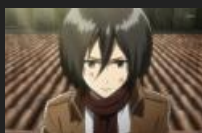
Find

👍 Add Thank You

Reply

Quote

Report



Luna ●

Administrator



Posts: 958

Threads: 0

Thanks

Received: 429

in 188 posts

Thanks Given:

241

Joined: Oct

2013

Reputation:

119



03-28-2016, 11:50 PM

#3

Quick Reply



Hades.y2k Wrote: →

(03-28-2016, 09:48 PM)

အမှန်အတိုင်းဝန်ခံရရင် post ကြီးပဲဖတ်တာဘာမှနားမလည်လိုက်ဘူး ဘရိုပြောသလို link မှာသွားတွက်ကြည့်မှပဲသဘောပေါက်လာတယ်
ဒါနဲ့အခုနောက်ပိုင်း AES Encryption လဲသုံးကြတယ်ဘရို NSA က classified information တွေကို AES 256 encryption နဲ့ပို့တယ်
တောင်ပြောတယ်
သိသလောက်လေးဝင်ဆွေးနွေးကြည့်တာ 😊

ဟုတ်ဘရို နောက်ပိုင်းလေ့လာဖြစ်ရင် ပြန်ရဲ့ပေးမယ်လေ ။ လောလောဆယ်တော့ RSA နဲ့ပတ်သတ်တဲ့ လေ့လာမှလေးတွေလုပ်လိုက်ဦးမယ်။
တစ်ခုခုလုပ်မှရမယ်။ Hee 🙄 Post ခုညီးပဲဖတ်ရင် နားမလည်ဘူးဗျ ဟုတ်တယ်။ ဂျာနောကလက်နဲ့ခုတွက်လိုက်ရတယ်။ ပြီးမှ တစ်ဆင့်
ခွင်းစမ်းလို့ရတဲ့ဟာကိုတွေ့တာ။ Mathematics Background ကို လိုက်ဖတ်နေရတာနဲ့ တော်တော်ကြာသွားတယ်။ အာနဲ့ Calculator တော့ရှိ
မှာပဲဆိုပြီး Google မှာရှာလိုက်တာ။ စာဖတ်တဲ့သူတွေအဖို့တော့ ပိုလွယ်သွားတာပေါ့။ 🤖

<http://www.thinbashane.wordpress.com>

Jabber : mrx@creep.im

PM

Find

Add Thank You

Reply

Quote

Report

« Next Oldest | Next Newest »

Enter Keywords

Search Thread

New Reply

Quick Reply





Quick Reply

Message
Type your reply to this message here.

☐ Disable Smilies

[Post Reply](#) [Preview Post](#)

 [View a Printable Version](#)

 [Subscribe to this thread](#)

Forum Jump:

-- Cryptography ▼

[Go](#)

Users browsing this thread: Hacke3erDD

Myanmar Security Forum (MSF) © 2013 - 2016 - All Rights Reserved.

Powered By MyBB, © 2002-2016 MyBB Group. — Theme by FlatInk LLC.
[Contact Us](#) — [Return to Top](#) — [Lite \(Archive\) Mode](#) — [RSS Syndication](#) | [Awards](#)