

Forum:[Hack Forums](#)

Thread: [\[Source\]\[VB.Net\]Asymetric RSA encryption example](#)

pr0t0typ3 - October 20, 2010, 1:09 pm

Asymetric RSA Encryption Example

Hey Today I gonna show you a little snippet I wrote to show you the usage of the RSA-Encryption which is included in the .net Framework.

This Encryption is a kind of different to almost everything you saw before.

It works with two keys. One you can make public that can only encrypt Text/Files/smith. else. And one key you should keep private as only this key can decrypt the encrypted data/text.

The special and very very good thing about that is, that you don't need a key exchange.

That means that if you make a RAT for example and the Victim is able to sniff the traffic he'll only get the encryption key which will not make it possible to decrypt the sending/sent data/text.

So here are the positive things about this encryption example:Secure (As much bit as you want (I used 512))

Asymetric (no keyexchange needed)

And here you go:

[img]http://img839.imageshack.us/img839/5351/2010v.png[/img]

And for all leechers:

[Pastebin](#)

Have Fun and post some Feedback.. It took me some time to make that...

Mr. Anderson - October 20, 2010, 1:11 pm

Awesome code :)

so this can go up to 1024 bits as well ?

iDope -.- - October 20, 2010, 1:11 pm

Going to go through the source now.

Thanks for this, looks like it'll help me somewhere.

The-Noob - October 20, 2010, 1:11 pm

very nice. I'm trying to learn about encryption and such :)

pr0t0typ3 - October 20, 2010, 1:23 pm

(Oct 20, 2010 01:11 PM)Mr. Anderson Wrote: [\[CITE\]](#) Awesome code :)

so this can go up to 1024 bits as well ?

You can go up to 10240 if you want ^^ as high as you want but it will become very slow and 512 should be enough

c6p0 - October 20, 2010, 1:25 pm

thanks add this in my crypter/binder

many thanks .

pr0t0typ3 - October 20, 2010, 1:29 pm

(Oct 20, 2010 01:25 PM)c6p0 Wrote: [\[CITE\]](#) thanks add this in my crypter/binder

many thanks .

No Problem..

I don't know if it is a good idea for a crypter as it is mainly used for very secure data (CIA and M16 are also using it) and a Crypter just needs to be undetected.

I would suggest it for a RAT as I already mentioned above.

Asus - October 20, 2010, 1:34 pm

Wow nice :) First metric RSA encryption seen here.

Times Change - October 20, 2010, 1:36 pm

Thanks, I will be using this to actually understand the encryption and probably try and make my own crypter.

pr0t0typ3 - October 20, 2010, 1:43 pm

(Oct 20, 2010 01:34 PM)Asus Wrote: [\[CITE\]](#) Wow nice :) First metric RSA encryption seen here.

No Problem.. Thanks for the feedback and @above I already said that I guess this is not the best encryption you could use for a crypter .. Maybe a HWID/Login System would be nice using this

6e756c6c - October 20, 2010, 1:58 pm

<https://hackforums.net/showthread.php?tid=680762>

Not trying to jack the thread or anything, just providing another resource for this. As Prototype has mentioned, you definitely do NOT want to use this for a crypter - it should be limited to small amounts of data (128 to 1,024 bytes).

pr0t0typ3 - October 20, 2010, 2:00 pm

Ah well I didn't see your thread but it is a kind of similar to my usage good work and yeah you should not use it in a crypter

c6p0 - October 20, 2010, 2:07 pm

these possible to divide the server into several parts so that each party is encrypted independently.

6e756c6c - October 20, 2010, 2:44 pm

No, Asymmetric encryption is intended to transfer a key so that said key can be used as a Symmetric encryption key. Never use it on large amounts of data.

c6p0 - October 20, 2010, 3:06 pm

ok thanks sir

just for little server like downloader .

H3x0S - October 20, 2010, 3:17 pm

Thank you for this very secure encryption example.

I have a one question. If I use a HttpRequest with POST data and encrypt the POST data with this encryption, can the username and password be sniffed?

Black-Blood™ - October 20, 2010, 3:41 pm

If I got it right it can't be sniffed cause only you've got the "silent" key.

Dolus - October 20, 2010, 5:03 pm

(Oct 20, 2010 01:29 PM)pr0t0typ3 Wrote: [\[CITE\]](#) CIA and M16 are also using it

Who exactly told you this?

6e756c6c - October 20, 2010, 5:15 pm

I have heard that quite a few times myself actually, apparently a lot of banks and the US military use RSA 2048 bit encryption. Which would make sense, since it's so secure and bruteforcing it would be very.. unlikely.

Grudgeee - October 20, 2010, 5:23 pm

Nice, Thanks for the source man!

Dolus - October 20, 2010, 5:32 pm

(Oct 20, 2010 05:15 PM)Aeonhack Wrote: [\[CITE\]](#) I have heard that quite a few times myself actually, apparently a lot of banks and the US military use RSA 2048 bit encryption. Which would make sense, since it's so secure and bruteforcing it would be very.. unlikely.

The UK security services encryption is not available to civilians.

pr0t0typ3 - October 20, 2010, 9:59 pm

(Oct 20, 2010 05:03 PM)DAM Wrote: [\[CITE\]](#) Who exactly told you this?They told it their selves after the 'Public RSA' was 'invented' in 1982 by americans. 2002 the M16 made the secret docuemnts about the last 40 years public and they said clearly that they already knew this encryption since 1962

(Oct 20, 2010 03:17 PM)H3x0S Wrote: [\[CITE\]](#) Thank you for this very secure encryption example. I have a one question. If I use a HttpRequest with POST data and encrypt the POST data with this encryption, can the username and password be sniffed?

Well if you use the same idea like common Wifi Networks do, there will be a RSA Provider at the client and at the server generated.

They send each other the public key and the modulus.

Now both of them can encrypt data using the public key of each other (which could also be sniffed but is useless as you can only bruteforce) and send the encrypted data to them.

The only on who has the private key to decrypt is the original source of the Public key that was used for encryption.

This will never be transfered so it can't be sniffed.

The only possibility to attack this secure connection is a 'Man in the Middle Attack' the 'hacker/sniffer' would catch all packets from the server and would save the public key sent by the server with and send a own fake key to the client.

The client would always post the data encrypted with the fake key and the 'hacker' could recive, decrypt, read and then reencrypt with the original public key and send to the server and so on.

(Oct 20, 2010 05:15 PM)Aeonhack Wrote: [\[CITE\]](#) I have heard that quite a few times myself actually, apparently a lot of banks and the US military use RSA 2048 bit encryption. Which would make sense, since it's so secure and bruteforcing it would be very.. unlikely.

It would take like a billion years if you use 2048 bits

pr0t0typ3 - October 21, 2010, 1:16 pm

little for smth. awesome ^^

Dolus - October 21, 2010, 2:47 pm

(Oct 20, 2010 09:59 PM)pr0t0typ3 Wrote: [\[CITE\]](#) They told it their selves after the 'Public RSA' was 'invented' in 1982 by americans. 2002 the M16 made the secret docuemnts about the last 40 years public and they said clearly that they already knew this encryption since 1962

M16? You mean SIS? I don't believe SIS has released the last 40 years of 'secret documents'. There has been some leaks by officers and some information which does not put anything or

anyone in imminent danger. Again the encryption which they use for the most secretive of files is not public and is hardware based.

S!rk0 - October 21, 2010, 3:16 pm

Good sharing ... Thank's Bro' ...

drizzy_effect - October 21, 2010, 4:58 pm

this looks very sexy nice job I hope that leecher's don't get this sniped

50GTB - October 28, 2010, 5:10 am

pr0t0typ3 is top fucking programmer here i would say

Asus - October 29, 2010, 5:15 pm

Used this, thanks :) Great stuff.

n0\$f3ratu\$ - November 6, 2010, 9:54 am

Thank you very much for the source. This made my stub UD. Is Detected only by avira now. Is till good i guess for a noob.

Thank you again pr0t0typ3.

H3x0S - November 6, 2010, 9:55 am

(Nov 6, 2010 09:54 AM)nosferatus Wrote: [\[CITE\]](#) Thank you very much for the source. This made my stub UD. Is Detected only by avira now. Is till good i guess for a noob.

Thank you again pr0t0typ3.

You shouldn't use it in crypter.

n0\$f3ratu\$ - November 6, 2010, 10:28 am

(Nov 6, 2010 09:55 AM)H3x0S Wrote: [\[CITE\]](#) You shouldn't use it in crypter.

Why not?

Is working.

Is getting the job done.

So... why not?

pr0t0typ3 - November 6, 2010, 10:38 am

It is slow and not good for large amounts of text/binary content

H3x0S - November 6, 2010, 10:39 am

(Nov 6, 2010 10:38 AM)pr0t0typ3 Wrote: [\[CITE\]](#) It is slow and not good for large amounts of text/binary content

How secure would this be in HWID systems?

n0\$f3ratu\$ - November 6, 2010, 10:40 am

I will send you in pm the link to my crypter so you can see is not loading hard or the ouput. Please take 1 minute and tell what you think. Your a great guy and i want your opinion. Thank you.

pr0t0typ3 - November 6, 2010, 1:36 pm

(Nov 6, 2010 10:39 AM)H3x0S Wrote: [\[CITE\]](#) How secure would this be in HWID systems?Very secure but you would need a implementation in PHP to use it properly

FamousMassacre - November 6, 2010, 2:42 pm

I feel nubish, why isnt this working?

```
TextBox1.Text = RSA.Encrypt(MyRSA.Exponent, MyRSA.Modulus, a)
```

pr0t0typ3 - November 7, 2010, 2:21 am

(Nov 6, 2010 02:42 PM)FamousMassacre Wrote: [\[CITE\]](#) I feel nubish, why isnt this working?

```
TextBox1.Text = RSA.Encrypt(MyRSA.Exponent, MyRSA.Modulus, a)
```

The Encrypt function is returning a Byte Array and a Textbox shows a String as Text so you would need to convert the Byte() to a String using the System.Text.Encoding.Default.GetString(Your Byte Array) Function. Also the Variable "a" you are encrypting has to be a Byte Array.

skyn_valdeur - November 7, 2010, 10:31 am

thanks man.. really in need for this.. thanks..

1 question, how to send the encrypted bytes via network socket..?

IonCore - November 7, 2010, 10:48 am

can u make a tut on this on how to apply this in a HWID system?

TheDubWubCub - March 12, 2011, 12:12 pm

ok, ive tried for about 2 hours now to get this WORKING! idc if you call me a noob but can someone just please help me! please PM me

pr0t0typ3 - March 13, 2011, 3:27 am

I included a whole source on how to use it in the original post

Air0x - March 13, 2011, 4:27 am

Well done pr0t0, you really know your stuff.

TheDubWubCub - March 13, 2011, 3:24 pm

can you please help me! :D

<http://img836.imageshack.us/img836/7210/helpme.png>

TheDubWubCub - April 22, 2011, 7:06 pm

can anyone help?! i will <3333

colorless - April 22, 2011, 11:13 pm

So would you just have the usual lof file stub bs just using this as the encryption method?