

Forum: [Hack Forums](#)

Thread: [Cryptography, Encryption, and Decryption - Create Subforum for Crypters](#)

sarciszewski - June 22, 2015, 7:31 pm

Most of the threads in the Cryptography, Encryption, and Decryption forum pertain to crypters; whose purpose is to evade antivirus detection and frustrate reverse engineering efforts.

This is a little disappointing. There is a wide and deep range of topics that can be discussed in the realm of cryptography, even outside the scope of ciphers and hash functions.

Information entropy

One Time Pads

Cryptographically secure randomness

Diffie Hellman key agreement schemes

Digital signature schemes

Block cipher modes of operation

Message Authentication Codes

AEAD constructions

Padding oracle attacks

Chosen plaintext attacks

Chosen ciphertext attacks

Stripping opportunistic encryption

Timing attacks

Cache-timing attacks (and other variants, e.g. FLUSH+RELOAD)

Twist-secure elliptic curve parameter choices

I propose all talk about Crypters (including the stickies) be migrated to a dedicated subforum of Cryptography, Encryption, and Decryption; and we focus the parent forum on this rich and diverse field of study.

d4rkj4y - June 22, 2015, 7:34 pm

I made a thread about this a while back.

<https://hackforums.net/showthread.php?tid=2045696>

It's a good idea, no doubt.

Niko - June 22, 2015, 7:36 pm

I like your Idea, I have thought about this a bit, It would be great.

OsLay - June 22, 2015, 7:37 pm

Great idea this would allow for more discussion on Cryptography instead of just threads asking what type of crypter to use and threads of that nature.

methodd - June 22, 2015, 7:48 pm

legit idea, very creative.

sarciszewski - June 22, 2015, 8:34 pm

(Jun 22, 2015 07:34 PM)d4rkJ4y Wrote: [\[CITE\]](#) I made a thread about this a while back.

<https://hackforums.net/showthread.php?tid=2045696>

It's a good idea, no doubt.Hah! Great minds think alike! (Feel free to PM me if you'd like to talk about cryptography stuff in a noise-free environment in the meantime.)

(Jun 22, 2015 07:36 PM)LegitBytes Wrote: [\[CITE\]](#) I like your Idea, I have thought about this a bit, It would be great.Thanks! :D

(Jun 22, 2015 07:37 PM)0651 Wrote: [\[CITE\]](#) Great idea this would allow for more discussion on Cryptography instead of just threads asking what type of crypter to use and threads of that nature. Cryptanalysis is a lot more fun than evading antivirus. (You often don't even need to encrypt to evade AV, and a dedicated reverse engineer will break your encryption anyway. It has to decrypt to execute!)

(Jun 22, 2015 07:48 PM)methodd Wrote: [\[CITE\]](#) legit idea, very creative.Thanks, but apparently it's not an original notion either. :)

Aiba - June 22, 2015, 8:35 pm

Noble of you but it will get denied :c

sarciszewski - June 22, 2015, 8:38 pm

(Jun 22, 2015 08:35 PM)Aiba Wrote: [\[CITE\]](#) Noble of you but it will get denied :c

Is there any particular reason you believe it will get denied? I believe this would be a vast improvement in the organization of topics on HN, and it's a rather simple change to the architecture. The benefit will be a better signal:noise ratio for people interested in cryptology, which leads to better communication and better relationships.

In short, the community as a whole will benefit from this choice.

GenericSkid - June 22, 2015, 8:40 pm

The section is cancerous but unfortunately it'll stay that way (edit: for awhile at least. May split later). Been suggested a few times before with lots of support.

sarciszewski - June 22, 2015, 8:43 pm

(Jun 22, 2015 08:40 PM)Lord Pankake Wrote: [\[CITE\]](#) The section is cancerous but unfortunately it'll stay that way. Been suggested a few times before with lots of support.Were any of these previous suggestions explicitly rejected? If so, what was the reason for the rejection? (If it's a lack of manpower, I'm willing to put some skin in the game and volunteer to help.)

crazyycast13 - June 22, 2015, 10:39 pm

We already got this suggestion approved, if you want to discuss things like this post threads into the

hashing and ciphers section.

<https://hackforums.net/showthread.php?tid=4828965> <-suggestion thread

sarciszewski - June 22, 2015, 10:53 pm

(Jun 22, 2015 10:39 PM)crazyycast13 Wrote: [\[CITE\]](#) We already got this suggestion approved, if you want to discuss things like this post threads into the hashing and ciphers section.

<https://hackforums.net/showthread.php?tid=4828965> <-suggestion thread

[Already did, actually](#), but...

My request is actually distinct from this one. I'd much rather see all of the crypter talk get moved into a subforum. Cryptography is much more than ciphers and hashes. See the list I gave in the OP for example.

crazyycast13 - June 22, 2015, 11:04 pm

(Jun 22, 2015 10:53 PM)binary_paroxysm Wrote: [\[CITE\]](#) [Already did, actually](#), but...

My request is actually distinct from this one. I'd much rather see all of the crypter talk get moved into a subforum. Cryptography is much more than ciphers and hashes. See the list I gave in the OP for example.

Read through the entire thread and see that I completely agree with you. I wanted something just for crypters, and what we have now is what we have now.

sarciszewski - June 22, 2015, 11:10 pm

(Jun 22, 2015 11:04 PM)crazyycast13 Wrote: [\[CITE\]](#) Read through the entire thread and see that I completely agree with you. I wanted something just for crypters, and what we have now is what we have now.

I see. You're right. I misunderstood your post.

???? - June 24, 2015, 8:04 am

Support the notion wholeheartedly.

Omniscient - June 24, 2015, 4:16 pm

Adjustments I have made will stand for now without further changes.