

Thomas Pornin

- Member for 14 years, 11 months Last seen more than a week ago



Activity

Stats

74,322	8.8m	540	1
reputation	reached	answers	question

About

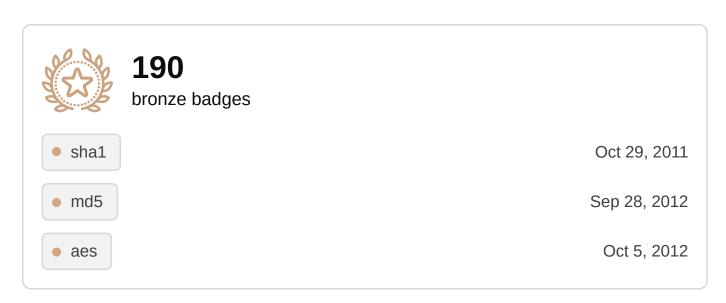
Cryptographer, programmer in several languages (C, Java, several assemblies, Pascal, Forth...). I also have a life.

Badges View all badges









Top tags View all tags

cryptography	1,870 score 111 posts	21 posts %
hash	1,813 score 94 posts	17 posts %
encryption	1,091 score 106 posts	20 posts %
c •	1,066 score 60 posts	11 posts %
java •	980 score 120 posts	22 posts %
security	738 score 53 posts	10 posts %

Top posts

View all questions, answers, and articles

All	Question	ns Answers Articles Score Newest	
A	527	Is it safe to ignore the possibility of SHA collisions in practice?	Oct 25, 2010
Α	444	Execution time of C program	Mar 9, 2011
A	255	Comparison of DES, Triple DES, AES, blowfish encryption for data	Apr 5, 2011
A	216	Is SHA-1 secure for password storage?	May 5, 2010
A	144	Is calculating an MD5 hash less CPU intensive than SHA family functions?	Apr 27, 2010
A	124	Is it possible to get identical SHA1 hash?	Mar 19, 2010
A	121	Garbage collector in Android	Jun 25, 2010
Α	115	Setting std=c99 flag in GCC	Feb 3, 2010
A	102	When generating a SHA256 / 512 hash, is there a minimum 'safe' amount of data to hash?	Jan 13, 2011
A	96	verifying a file signature with openssl dgst	Mar 5, 2010

Top Meta posts





Swap TLS and SSL tags?

Top network posts

View all network posts



1213

How to securely hash passwords?



698

How does SSL/TLS work?



674

Do any security experts recommend bcrypt for password storage?



606

CRIME - How to beat the BEAST successor?



570

What's the difference between SSL, TLS, and HTTPS?

Communities

View all [7]



Information Security 328.7k

Cryptography 87.9k



Stack Overflow 74.3k



History 5.3k



Space Exploration

1.5k