**cs387 Office Hours**

**Alastair Aitchison asks:**

Would it be possible for Professor Evans to suggest any suitable reading material for those not so familiar with some of the maths and symbology used in Unit 3?

For example, what does the group Z\_q mean?

[link](http://forums.udacity.com/cs387-april2012/answer_link/2440/)|[award points](http://forums.udacity.com/cs387-april2012/award_points/user/2765/answer/2440/)|[edit](http://forums.udacity.com/cs387-april2012/answers/2440/edit/)|[delete](http://forums.udacity.com/cs387-april2012/delete/2440/)|more ▼

answered **03 May, 10:47**

lastair%20Aitchison's gravatar image

[Alastair Ait...](http://forums.udacity.com/cs387-april2012/users/2765/alastair-aitchison)  
**334**●4

**Fernando asks:**

1. Regarding D-H key distribution, Is there any restriction on the range of A or B, chosen by Alice and Bob? Seems to me that they should be less that p (the prime number), but not sure.

[ Good question – large numbers, but not related to p, other than similar security level. > 256 bits is recommended- there are attacks that require sqrt(a) work, so having 256 bits in a is comparable to a 128-bit key. ]

Fernando also asks:

1. Why RSA seems to have a much more acceptance (in practice) than D-H? Just wanted to know if there are any know vulnerability with D-H.

Thanks very much.

[link](http://forums.udacity.com/cs387-april2012/answer_link/2328/)|[award points](http://forums.udacity.com/cs387-april2012/award_points/user/2156/answer/2328/)|[edit](http://forums.udacity.com/cs387-april2012/answers/2328/edit/)|[delete](http://forums.udacity.com/cs387-april2012/delete/2328/)|more ▼

answered **01 May, 17:33**

ernando's gravatar image

[Fernando](http://forums.udacity.com/cs387-april2012/users/2156/fernando)  
**176**●2

**Megan Stewart asks:**

I had a recent run-in with a company that produces e-books, related to the fact that I'm unwilling, for security reasons, to store my credit card number on the company's website in order to download e-books. After doing a google search, I stumbled on a comment by somebody claiming this company's copyright scheme entails using the customer's credit card number as a key to encrypt the e-book. On the plus side, according to the comment, you were free to share the e-book with others, as it was easy to assure the book wasn't pirated.

[link](http://forums.udacity.com/cs387-april2012/answer_link/2446/)|[award points](http://forums.udacity.com/cs387-april2012/award_points/user/4272/answer/2446/)|[edit](http://forums.udacity.com/cs387-april2012/answers/2446/edit/)|[delete](http://forums.udacity.com/cs387-april2012/delete/2446/)|more ▼

answered **03 May, 12:38**

egan%20Stewart's gravatar image

[Megan Stewart](http://forums.udacity.com/cs387-april2012/users/4272/megan-stewart)  
**45**●1

**[ really bad idea. .. watermarking scheme ]**

**Several people asked questions about the challenge problem for Unit 2-6 not being hard enough. What happened?**

vipuldiyyanshu asks:

Could Professor Evans give the **method of solving (tips and techniques and materials to refer to improve our practical cryptoanalyst skills and solution) the challenge problems** at the end of the course before the final exam so that we can have and idea of how to approach these problems practically rather than just knowing the theoretical approach only. It will be a great help because i have spent many frustrating hours to solve them and with my current experience and knowledge i wasn't happy with the outcomes .

Thank you.

[link](http://forums.udacity.com/cs387-april2012/answer_link/2636/)|[award points](http://forums.udacity.com/cs387-april2012/award_points/user/620/answer/2636/)|[edit](http://forums.udacity.com/cs387-april2012/answers/2636/edit/)|[delete](http://forums.udacity.com/cs387-april2012/delete/2636/)|more ▼

answered **yesterday**

ipuldivyanshu's gravatar image

[vipuldivyanshu](http://forums.udacity.com/cs387-april2012/users/620/vipuldivyanshu)