Homework 7

1. What are good uses of anonymity services like Tor?

2. What is meant by the notion *forward privacy*?

3. What is a *re-identification attack*?

4. Imagine you have a completely 'innocent' email message, like birthday wishes to your grandmother. Why should you still encrypt this message and your grandmother take the effort to decrypt it?

   (Hint: The answer has nothing to do with preserving the privacy of your grandmother and nothing to do with keeping her birthday wishes super-secret. Also nothing to do with you and grandmother testing the latest encryption technology, nor just for the sake of it.)

5. One part of achieving privacy (but not the only one) is to properly encrypt your conversations on the Internet. But this is fiercely resisted by some spy agencies. These agencies (and some politicians for that matter) argue that, for example, ISIL's recruiters broadcast messages on, say, Twitter, and get people to follow them. Then they move potential recruits to Twitter Direct Messaging to evaluate if they are a legitimate recruit. If yes, they move them to an encrypted mobile-messaging app. The spy agencies argue that although they can follow the conversations on Twitter, they "go dark" on the encrypted message app. To counter this "going-dark problem", the spy agencies push for the implementation of back-doors in iMessage and Facebook and Skype and everything else UK or US-made, which they can use eavesdrop on conversations without the conversants' knowledge or consent.

   What is the fallacy in the spy agencies going-dark argument? (Hint: Think what would happen if the spy agencies and certain politicians get their wish.)