**Identity and Authentication**

**CRYPTO LITERACY**

* Stargate-Ghost problem: Two people communicating through an untrusted medium. How can they communicate effectively?
  + Do we need communication to be encrypted? **Confidentiality**
  + It is a potential exam question.
* Sitting in a locked room getting bits.
  + You are locked away somewhere and you can’t talk with anyone. You just have a computer screen and text is coming in on the screen. You cannot interact with reality at all.
  + The only way to talk to him in the featureless room with no windows etc. is a little screen in front of him and we can send messages to him on a screen / he can type message back to us.
  + He gets a message, which says “can you tell me where you left the keys of the house”, “I’m locked out, it’s your mum”.
  + **Problem: is what is being said true? Is it really his mum? The problem of authentication**.