5.1 Signatures and hash (Reading for Interest)

Digital signature actually plays a large role in real life applications (so too does hashes if you consider that the hash creates the short digest from the message that is signed).

Many countries in the world assign Digital Signature the same important legally as hand signatures. For example, in Hong Kong the Electronic Transaction Ordinance states that digital signatures is a considered a valid signature if “it is reliable, appropriate and agreed by the recipient of the signature”. This means the parties must agree to use it and the algorithm must be accepted as appropriate.

http://www.ogcio.gov.hk/en/regulation/eto/

In the lecture I also briefly mention the speeding fine that was cancelled because the offender had brought into question the integrity of the hash function used (MD5 - on which collisions could be found). You can read more about it here (it was in 2005 and a similar argument will likely fail today).

NSW speed cameras in doubt - National - theage.com.pdf

MD5 flaw pops up in Australian traffic court - CNET.pdf

As this was the last lecture with algorithms I just wish to remind you that it is important to have a basic understanding of algorithms, however it is unlikely that many of you will implement them. Using these will most often require you to use and apply the correct libraries, like for example:

http://developer.android.com/reference/javax/crypto/package-summary.htmlLinks to an external site.

https://www.openssl.org/

However, given what you learnt you should be able to choose the better algorithms and understand what services to use these for.

Finally, if you are more interested looking at things from a system security perspective you should remember that it does not matter if your cryptographic methods are good if your code is bad…

https://www.imperialviolet.org/2014/02/22/applebug.html