3.1 Number Theory and Practical Security (Interest Only)

Some people think that cryptographic algorithms and the underlying mathematics are mostly theoretical with little practical use. It is true that if you work in security, it is unlikely that someone asks you do design an algorithm like AES or RSA (and you should not do so really as there are enough good algorithms to use).

However, it is still important to have basic knowledge of how algorithms work at low level. A very practical area of security that is all about low level implementation of algorithm is side channel analysis. This is the idea that observing the device during calculation of algorithm can give us and idea what it is calculating. This is especially problematic if we are doing cryptographic calculation with secret/private keys.

I briefly told you about this in the lecture but this video also gives a good idea of some basic use of side channel (it is the issue surrounding RSA and square and multiply algorithm, they also mention Chinese Remainder Theorem)

https://www.rambus.com/side-channel-analysis-demo-mobile-device/

Side channel analysis can also be used other algorithms, for example AES (then it is not square and multiply, but inner working of the substitution/permutation):

https://www.youtube.com/watch?v=l5Oi9xNR60s&feature=emb_rel_end/

(Side note: Cryptography Research (now Rambus) was started by some guys who discovered differential power analysis and made some countermeasure for it - this made a lot of money as at the time everyone who made any crypto processor (e.g. every credit card with chip) had to pay them to use their idea. So very practical knowledge...)