

## 4.1 Question 1

### 4.1.A Provide a quick explanation for the statements that are FALSE:

**The principle requirement of PRNG is that the generated number stream be unpredictable.**

True

**With true random sequences each number is statistically independent of others and therefore unpredictable.**

True

**The pseudorandom number generator may simply involve conversion of an analog source to a binary output.**

**False**, this is only true for a **true** random number generator, as can be seen on slide 7 from the lecture.

**Examples of a pseudorandom function are decryption keys and nonces.**

False,

**A widely used technique for pseudorandom number generation is an algorithm known as the linear congruential method.**

True

**The security of Blum, Blum, Shub is not based on the difficulty of factoring  $n$ .**

**False**, it is dependant on the fact the factoring  $n$  is difficult.