Deniz Aytemiz

Q1. Multiple Choice Questions

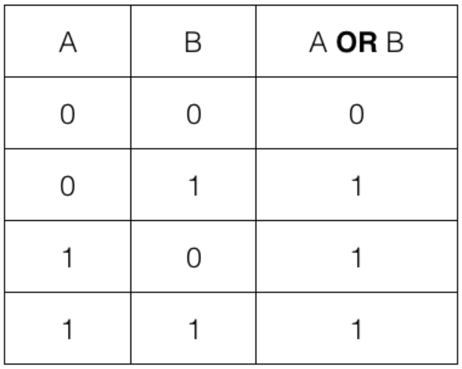
1. A
2. B
3. D
4. B
5. B

Q2. Encryption & Random Number Generation

I. A deterministic RNG consists of an algorithm that produces a sequence of seemingly random bits from an initial value called seed. A nondeterministic RNG produces output dependent on some unpredictable physical source that is not human dependent . TRNG is a nondeterministic RNG whose source comes from true randomness. It can be an analog to digital converter for instance. It creates a random bit stream. PRNG is a deterministic algorithm. It has seed as the initialization of the algorithm and creates a pseudorandom bit stream which is not truly random but seemingly random.

II. PRNG must be used for the random bit stream that will be XOred with the input bit stream because the system should be able to have/generate random bit continuously without any dependence on the outside source. So if TRNG is used the entropy pool can empty at some point and the system may not be able to generate random bits. For the creation of the IV on the other hand since it does not require continuous production and you need only 1 IV in the whole process, TRNG can be used and having a truly random IV would increase the security of the system significantly.

III. If X is a uniform random variable then, P(X=0)=P(X=1)= 0.5 and it is the same with Y. Therefore, looking at the OR table of 2 bits:



A	B	A **OR** B
0	0	0
0	1	1
1	0	1
1	1	1

There is 0.25 probability of the outcome being 0 and 0.75 being 1. Therefore the probability is not uniformly distributed among the possible outcomes. Hence it is not an uniformly distributed random variable.

Q3. Extra Credit

The entropy source of a TRNG can be from the physical environment of the computer for instance, keystroke timing patterns, disk electrical activity, mouse movements.Also unpredictable natural processes such as pulse detectors of ionizing radiation events, gas discharge tubes, and leaky capacitors.

Hardware sources as such can be biased in some way such as having one bit more than other in the stream. So the usual approach is to assume there is some bias and apply techniques for randomizing the bits. These methods are referred to as conditioning algorithms or deskewing algorithms.