# Tutorial 12: Hash Functions

1. Search on the internet and determine a solution for the problem of the birthday paradox:
    a. How many people do you need before the odds are good (greater than 50%) that at least two people in the same room share the same birthday.
    b. Revisit the problem assuming that there are a 1000 days in the year.
        i. How many people must be in the room to have a better than 50% chance that one of them share a birthday with you.
        ii. How many people must be in the room to have better than 50% chance that two of them share the same birthday? This problem should be approached with some probability and a Matlab program.

2. If a programming solution to question 1 is taken, verify that (using a few different values for number of days in a year that:
   (Num people required) is proportional to sqrt(Num days in year)

3. How many hash calculations would be required to launch a birthday attack on a hash of length 160 bits?

4. Find and read material on SHA and HAVAL.

5. Some hash functions also have a key input so that in addition to generating a one-way hash information, the correct key is also required to generate and verify the hash. Hashes produced this way are called Media Access Codes (MAC). Provide a short description of how such a systems works and incorporates the key into the system.
6. What are the two most important properties of a secure hash function?

7. With reference to hash algorithms, explain what the birthday attack is and how the threat of this attack affects the choice of a hash algorithm’s hash size. No probability calculation is required. *[6 marks, Exam 2001]*

8. Refer to the diagrams of MD5. Use the tables to complete the first iteration of the first round, up to the input of the shifting stage only, using the plaintext block given below. Only the least significant byte of the result is required.

```
23FF A493  5B90 B1E8 2C8A F924 BA5C 3267 B2AC 0126 6CA5 78BA
6679 5580 DF89 AF66 6DCO 53DD 38AC 3D86 AE93 6494 3BFE BD49
B68A 0655 D579 21F7 15CB B22C 1BE7 BBC6
```

*[9 marks,Exam 2001]*

9. MD5 assumes a little-endian architecture. What is a little endian architecture, on what current computing platform is it popular? What is big-endian? A digest function must be independent of the underlying architecture and some detection and changes are required to operate on these platforms. Consider this in the application of these algorithms.