# 4 Number Theory and Cryptography

## 4.2 Integer Representations and Algorithms

1. This section presents techniques for transforming numbers from one base to another.

2. Base $b$ expansions of $n$: $n = a_k b^k + a_{k-1} b^{K-1} + \ldots + a_1 b^1 + a_0$

3. Example: 237 in decimal representation is $(237)_{10} = 2 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$
   Similarly 9 in binary is $(1001)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$

4. Binary (base 2) expansions of integers are bit strings that represent the particular integers, and they are used by computers to represent and do arithmetic with integers

5. Hexadecimal expansion of also used by computer. It uses $0, 1, \ldots, 9, A, B, C, D, E, F$

6. Bytes are bit strings of length 8

7. Base conversion (expressing $n$ base $b$):

   - $n = bq_0 + a_0$ $(0 \leq a_0 < b)$ and $a_0$ is the rightmost digit of $n$ base $b$
   - $q0 = bq1 + a1$ $(0 \leq a_1 < b)$ and $a_1$ is the 2nd digit from the right of $n$ base $b$
   - repeat to find $a_2, a3$, until $q_i = 0$ for some $i$

8. Converting from binary to/from hexadecimal: each hexadecimal digit corresponds to a block of 4 digits