16-124-836
Marcel Matti ZAUDER

4.3 Question 3

4.3.A State the value of the padding field in SHA-512 if the length of the message is:

5000 bits

1. Calculate size of the data in the last block:
$$5000 \; mod \; 1024 \; = \; 904$$
2. Add the size of the length field (128 bit) to the last block size:
$$904 + 128 \; = \; 1032$$
3. Because $1032 > 1024$ the last block is now:
$$1032 \; mod \; 1024 \; = \; 8$$
4. The length of the padding field is therefore:
$$1024 - 8 \; = \; 1016 \; bits$$
5. Therefore the padding consists of one 1 and 1015 zeros, hence the value is:
$$Value \; of \; Padding: \; 2^{1015}$$

5001 bits

1. Calculate size of the data in the last block:
$$5001 \; mod \; 1024 \; = \; 905$$
2. Add the size of the length field (128 bit) to the last block size:
$$905 + 128 \; = \; 1033$$
3. Because $1032 > 1024$ the last block is now:
$$1033 \; mod \; 1024 \; = \; 9$$
4. The length of the padding field is therefore:
$$1024 - 9 \; = \; 1015 \; bits$$
5. Therefore the padding consists of one 1 and 1014 zeros, hence the value is:
$$Value \; of \; Padding: \; 2^{1014}$$

5002 bits

1. Calculate size of the data in the last block:
$$5002 \; mod \; 1024 \; = \; 906$$
2. Add the size of the length field (128 bit) to the last block size:
$$906 + 128 \; = \; 1034$$
3. Because $1032 > 1024$ the last block is now:
$$1034 \; mod \; 1024 \; = \; 10$$
4. The length of the padding field is therefore:
$$1024 - 10 \; = \; 1014 \; bits$$
5. Therefore the padding consists of one 1 and 1013 zeros, hence the value is:
$$Value \; of \; Padding: \; 2^{1013}$$

4.3.B State the value of the length field in SHA-512 if the length of the message is:

5000 bits

0x0000000000000000000000000000001388

5001 bits

0x0000000000000000000000000000001389

5002 bits

0x000000000000000000000000000000138A