

# TTM4135 Worksheet 4: Hashing, MACs and Number theory

Tjerand Silde and Emil August Hovd Olaisen  
{tjerand.silde, emil.august.olaisen}@ntnu.no

Spring 2026

1. Review the definitions of the following concepts:
  - (a) collision resistance, second preimage resistance and one-wayness;
  - (b) birthday paradox;
  - (c) HMAC;
  - (d) GCM mode;
  - (e) big O notation;
  - (f) Fermat test;
  - (g) Miller–Rabin test.
  - (h) factorization and discrete logarithm problems.
2.
  - (a) Suppose that 10 items are chosen randomly (with replacement) from a set of 30 items. Find the probability that there is no collision (or, in other words, all the items are different). (Hint: consider the experiment one item at a time and multiply the probability that there is no collision each time.)
  - (b) Explain why SHA-256 can be said to match the security of AES with 128-bit keys.
3. A rough, but simple, estimate for the probability  $p(n)$  of obtaining one or more collisions when choosing  $n$  items (with replacement) from a set of  $H$  items is:

$$p(n) \approx \frac{n^2}{2H}.$$

Use this formula to estimate the probability of finding a collision in SHA-256 after  $2^{128}$  trials, after  $2^{100}$  trials, and after  $2^{80}$  trials.

4. When does the addition of the padding and length field in the SHA-2 family of hash functions result in an extra block to be processed?  
Consider, for example, a SHA-2 variant with 1024-bit blocks (such as SHA-512) and a message  $m$  of between  $(l - 1) \times 1024$  bits and  $l \times 1024$  bits. The message, after adding padding and the length field, is either  $l$  blocks or  $l + 1$  blocks. Exactly how long can the message be before  $l + 1$  blocks will be used?
5. Suppose that HMAC is implemented using a hash function  $H$ , where  $H$  is an iterated hash function with compression function  $h$ .
  - (a) How many additional applications of the compression function  $h$  are required to compute the MAC of a message  $m$ , in comparison with computing only  $H(m)$ ?
  - (b) If a MAC tag is to be computed for many different messages but the same key, how can pre-computation be used to reduce this overhead?
6. Consider the following simplification of HMAC, defined from any Merkle-Damgård hash function  $H$ :

$$\text{HMAC}'(m, K) = H(K \parallel m).$$

Show that this variant allows an attacker to forge a new valid MAC tag given any valid message/tag pair  $(m, T)$  by extending  $m$  to a new message  $m'$  and finding a valid tag  $T'$  for  $m'$ .

7. If possible, solve for the following equations for  $x$  using the Chinese Remainder Theorem (CRT). If they do not have a solution, then explain why.
- (a)  $x \equiv 5 \pmod{7}$  and  $x \equiv 7 \pmod{10}$ .
  - (b)  $x \equiv 3 \pmod{7}$  and  $x \equiv 7 \pmod{14}$ .
  - (c)  $x \equiv 2 \pmod{6}$  and  $x \equiv 3 \pmod{11}$ .
  - (d)  $x \equiv 8 \pmod{9}$  and  $x \equiv 11 \pmod{15}$ .
8. Find  $\phi(n)$  for all integers between 20 and 25 inclusive.
9. Find the discrete logarithm of the number 3 with regard to base 2, for the following moduli:
- (a) modulus  $p = 5$ ;
  - (b) modulus  $p = 11$ ;
  - (c) modulus  $p = 29$ .
10. Use the Fermat test to check whether the following numbers are prime or not. Run the test at most 4 times.
- (a) 979;
  - (b) 983.
11. (a) Show that the Carmichael number  $n = 1105$  passes the Fermat test for base  $a = 2$  and  $a = 3$ .
- (b) Now try the Miller–Rabin test for the same two bases and show that  $n$  is composite.
- (c) Hence find a square root of 1 mod  $n$  and use this to find a factor of  $n$ .