Tutorial -6

SOEN-321

Hash Function

One-way function
There is no H^{-1}

$$H(x) = y$$

Arbitrary length input
- Message
- Pre-image

Short fixed length output
- Hash code
- Hash value
- Message digest

Application: Hash Tables with O(1) lookup

Pigeonhole principle

- If n items are put in m containers where $n > m$, then at least one of the containers has more than one item

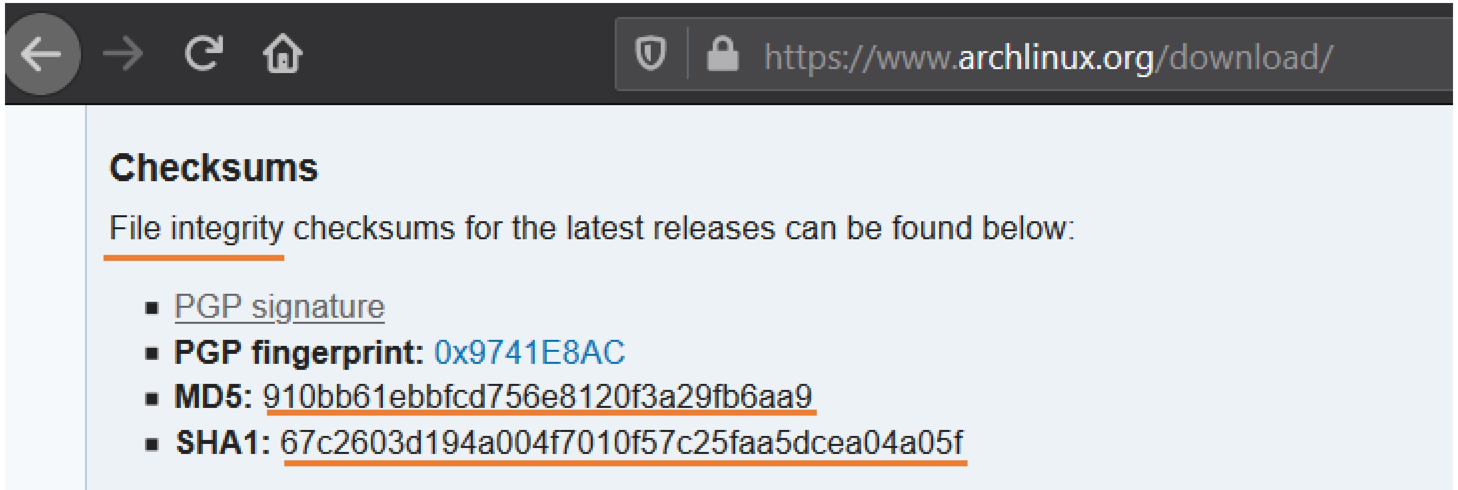
- It means, there must exist "collision"
  $H(x_1) = H(x_2), where\ x_1 \neq x_2$

Cryptographic Hash Function

1. Pre-image resistance
   - $Given\ y, it\ is\ hard\ to\ find\ x\ such\ that\ H(x) = y$
2. Weak collision resistance
   - $Given\ x_1, it\ is\ hard\ to\ find\ x_2\ such\ that\ H(x_1) = H(x_2)\ and\ x_2 \neq x_1$
3. Strong collision resistance
   - $it\ is\ hard\ to\ find\ any\ (x_1, x_2)\ such\ that\ H(x_1) = H(x_2)$

Examples: MD5, SHA1, SHA2, SHA3

Cryptographic Hash Function



Exercise 5-1

Bob is a paranoid cryptographer who does not trust dedicated hash functions such as SHA1 and SHA-2. Bob decided to build his own hash function based on some ideas from number theory. More precisely, Bob decided to use the following hash function:

H(m)= m^2 mod n,   n= p × q, where p and q are two large distinct primes.

Does this hash function satisfy the one-wayness property? What about collision resistance? Explain.

1- Pre-image resistant:

Yes, since p and q are secret, then finding the square root $mod\ n$ is a hard problem

2-Weak collision resistant

No, since for any given input m, the attacker can get the same hash value using input $-m$

3-Strong collision resistant

No, it is easy to choose any pair $(m, -m)$ which yields the same hash

Exercise 6-1

Let x=111 and y=19301. Factor n=21311 using the fact that $x^2 \equiv y^2 \; mod \; n$.

$x^2 - y^2 \equiv 0 \; mod \; n$

$(x+y)(x-y) \equiv 0 \; mod \; n$

If n divides $(x+y)(x-y)$, then they share common factors

$\gcd(x \pm y, n) = p \; or \; q$

$\gcd(111 + 19301, 21311)$

$\gcd(19412, 21311)$

$21311 = 19412 + 1899$

$19412 = 10 \times 1899 + 422$

$1899 = 4 \times 422 + 211$

$422 = 2 \times 211 + 0$

$\gcd(19412, 21311) = p = 211$

$q = \frac{n}{p} = \frac{21311}{211} = 101$