Problem Set 6

Alex Miller

November 18, 2021

Abstract

Collaborators: Elizabeth Coble, Lucy Li

1 1

Even if the loop exits after 2^{64} iterations, and is therefore computationally feasible for a well equipped adversary, the hash table would by that point take up 2^{64} space, which is too large to be considered feasible for even a well equipped adversary.

2 2

2.1 a

$h_1(x, v) = E(x, v) \oplus x$
$h_1(x, v) = E(x, v) \oplus x \oplus 0^B$
$h_1(x, v) = E(0^B, E^{-1}(0^B, E(x, v) \oplus x)) \oplus 0^B$
$h_1(x, v) = ch_1(x' = 0^B, v' = E^{-1}(0^B, E(x, v) \oplus x))$

2.2 c

$h_3(x, v) = E(0^B, x \oplus v) \oplus x$
$h_3(x, v) = E(0^B, x \oplus v) \oplus x \oplus 0^B$
$h_3(x, v) = E(0^B, E^{-1}(0^B, E(0^B, x \oplus v) \oplus x) \oplus 0^B) \oplus 0^B$
$h_3(x, v) = h_1(x' = 0^B, v' = E^{-1}(0^B, E(0^B, x \oplus v) \oplus x))$

3 3

Let **B** describe the input space of the hash function

Algorithm 1: $A(k, y)$

$m[1] \leftarrow \$\mathbf{B}$
$h' \leftarrow E(m[1], k)$
for $i = 1 ... \sqrt{B} - 1$ **do**
  $m[2] \leftarrow \$\mathbf{B}$
  if $h' = E^{-1}(m[2], y)$ **then**
    return $m[1] || m[2]$
  end
end
return $\perp$

$Pr[Expt_H^{pr}(A) = 1] = 1$:

Since E and E^{-1} have uniformly random output for a given key, we can define a target intermediary hash $h' = E(m[1], k)$, where $m[1]$ is a random B-bit value input and k is a random B-bit key. We can use this target value h' to try and find a hood value of $m[2]$ s.t. $h'' = E(m[2], y), h' = h''$. By the birthday principle, since h' and h'' are uniformly random integers $\in \{0, 1\}^B$, the probability we generate h'' s.t. $h'' = h'$ in $\sqrt{B}$ samples is $\approx \frac{\sqrt{B}^2}{B} = \frac{B}{B} = 1$

Therefore $Adv_H^{pr}(A) = Pr[Expt_H^{pr}(A) = 1] = 1$

A runs in $2^{\sqrt{B}} < 2^B$ time.

4 5

4.1 c

Counter Example: $a = 450, b = 300$. a and b are valid for our first relation.

$2a = 2bmod100 \Leftrightarrow 100|2(450 - 300)$
$2a = 2bmod100 \Leftrightarrow 100|300$

But these values of a and b do not make it so $a = bmod100$:

$a = bmod100 \Leftrightarrow 100|450 - 300$
$a = bmod100 \Leftrightarrow 100|150$

but 100 does not divide 150.

4.2 f

True:

$\exists c \in \mathbf{Z} ac = 1modN \Leftrightarrow gcd(a, N) = 1$
$\exists c \in \mathbf{Z} bc = 1modN \Leftrightarrow gcd(b, N) = 1$

Therefore we can say that neither a nor b share prime factors with N; in that case ab should not share prime factors with N, so:

$gcd(ab, N) = 1 \exists c \in \mathbf{Z} abc = 1modN$

Therefore ab is invertible modulo N

4.3 h

$(N - 1)$ is invertible modulo N:

$N - 1$ and N are relatively prime so $gcd(N - 1, N) = 1 \Leftrightarrow \exists c \in \mathbf{Z}(N - 1)c = 1modN$, which means $(N - 1)$ is invertible modulo N

Since $(N - 1)c = 1modN \Leftrightarrow N|(N - 1)c - 1$, we can find a good value for c by considering what would make N a divisor for $(N - 1)c - 1$. If $c = (N - 1)$ then $N|(N - 1)(N - 1) - 1 = N^2 - 2N + 1 - 1 = N^2 - 2N$. $N|N^2 - 2N \Leftrightarrow \exists k, N * k = N^2 - 2N$, and in this case k can $= (n - 2)$ (this hold because $N - 2 = k > 0$)

Therefore $N - 1$ is the inverse of $N - 1$ modulo N