Homework Set 11

Problem 1

Example 27. Consider the following compression function $C(x)$ which takes three bits input and outputs two bits:

x	000	001	010	011	100	101	110	111
$C(x)$	10	00	11	01	01	10	00	11

Let $H(x)$ be the hash function obtained from $C(x)$ using the Merkle–Damgård construction (using initial value $h_1 = 0$). Compute $H(11000)$.

Solution. Here, $b = 2$ and $c = 1$, so that each x_i is 1 bit: $x_1x_2x_3x_4x_5 = 11000$.
$h_1 = 00$
$h_2 = C(h_1, x_1) = C(001) = 00$
$h_3 = C(h_2, x_2) = C(001) = 00$
$h_4 = C(h_3, x_3) = C(000) = 10$
$h_5 = C(h_4, x_4) = C(100) = 01$
$h_6 = C(h_5, x_5) = C(010) = 11$
Hence, $H(11000) = h_6 = 11$.

Problem 2

Example 28. Bob's public RSA key is $(N, e) = (35, 19)$. His private key is $d = 19$. For signing, Bob uses the (silly) hash function $H(x) = x \pmod{22}$. Determine Bob's signature s of the message $m = 361$.

Solution. $H(m) = 361 \pmod{22} = 9$. The signature therefore is $s = H(m)^d \pmod{N} = 9^{19} \equiv 9 \pmod{35}$.

Problem 3

Example 29. Alice uses an RSA signature scheme and the (silly) hash function $H(x) = x_1 + x_2$, where $x_1 = 3x \pmod{11}$ and $x_2 = 2x \pmod{29}$, to sign the message $m = 1299$ with the signature $s = 121$. Forge a second signed message.

Solution. Since we have no other information, in order to forge a signed message, we need to find another message with the same hash value as $m = 1299$. From our experience with the Chinese remainder theorem, we realize that changing x by $11 \cdot 29$ does not change $H(x)$. Since $1299 + 11 \cdot 29 = 1618$, a second signed message is $(1618, 121)$.

Problem 4

Example 30. Among 20 people (no leaplings), what is the probability that two have the same birthday?

Solution. The probability is

$$1 - \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\left(1 - \frac{3}{365}\right)\cdots\left(1 - \frac{19}{365}\right) \approx 0.411438.$$

[Or, equivalently, about 41.14%.]

Armin Straub
straub@southalabama.edu

Problem 5

Example 31. Consider the elliptic curve $y^2 = x^3 + 3x + 5$ as well as the points $P = (4, 9)$ and $Q = (1, 3)$ on that curve. Determine $P \boxplus Q$.

Solution. We let Sage (you can use the input box on our course website!) do the work for us:

```
>>> E = EllipticCurve([3,5])
>>> E(4,9) + E(1,3)
```

$$(-1 : 1 : 1)$$

We conclude that $P \boxplus Q = (-1, 1)$ (the first two values).

Problem 6

Example 32. Consider the elliptic curve $y^2 = x^3 + 7x + 4$ as well as the point $P = (0, 2)$ on that curve.

(a) Determine $2P$.

(b) Determine $3P$.

Solution. We let Sage do the work for us:

```
>>> E = EllipticCurve([7,4])
>>> 2*E(0,2)
```

$$\left(\frac{49}{16} : -\frac{471}{64} : 1\right)$$

```
>>> 3*E(0,2)
```

$$\left(\frac{15072}{2401} : \frac{2021734}{117649} : 1\right)$$

We conclude that $2P = \left(\frac{49}{16}, -\frac{471}{64}\right)$ and $3P = \left(\frac{15072}{2401}, \frac{2021734}{117649}\right)$.

Problem 7

Example 33. Consider the elliptic curve $y^2 = x^3 + 3x + 2$ modulo 5. List all points (x, y).

Solution. Note that, because we are working modulo 5, there are only 5 possible values for x. Hence, we can go through all possibilities for x and determine the corresponding possible values for y:

- $x = 0$: $y^2 = 0^3 + 3 \cdot 0 + 2 = 2$ has no solutions.
- $x = 1$: $y^2 = 1^3 + 3 \cdot 1 + 2 \equiv 1$ has solutions $y \equiv \pm 1$, resulting in the points $(1, \pm 1)$.
- $x = 2$: $y^2 = 2^3 + 3 \cdot 2 + 2 \equiv 1$ has solutions $y \equiv \pm 1$, resulting in the points $(2, \pm 1)$.
- $x = -2$: $y^2 = (-2)^3 + 3 \cdot (-2) + 2 \equiv -2$ has no solutions.
- $x = -1$: $y^2 = (-1)^3 + 3 \cdot (-1) + 2 \equiv -2$ has no solutions.

Overall, we have found the points $(1, \pm 1)$, $(2, \pm 1)$, for a total of 5 points if we include the special point O.

Sage. Alternatively, we can let Sage do this work for us:

```
>>> E = EllipticCurve(GF(5), [3,2])
>>> E.points()
```

$[(0:1:0), (1:1:1), (1:4:1), (2:1:1), (2:4:1)]$

Problem 8

Example 34. Consider the elliptic curve $y^2 = x^3 + 9x + 5$ modulo 43 as well as the point $P = (3, 4)$ on that curve.

(a) Determine $2P$.

(b) Determine $3P$.

Solution. We let Sage do the work for us:

```
>>> E = EllipticCurve(GF(43), [9,5])
>>> 2*E(3,4)
```

$(25:26:1)$

```
>>> 3*E(3,4)
```

$(16:26:1)$

We conclude that $2P = (25, 26)$ and $3P = (16, 26)$.