Hashing and authentication ungraded homework

This homework is ungraded. Its purpose is to help you understand course material. Doing these problems may help you with your graded homework and quiz. Problems like these may appear on the midterm or final. You should attempt to complete them before the end of the module (time permitting), and at a minimum study them and their provided solutions.

1. Write one of the following reductions: from PreimageFinder(H,y) to 2ndPreimageFinder(H,x), or from 2ndPreimageFinder(H,x) to PreimageFinder(H,y). What security implication does your reduction establish?
2. Recall that you can compute a value that is equivalent to x mod (2^a - b) as (x div 2^a) · b + (x mod 2^a). Use this fact to reduce (base-10) 123456789 mod (2^{12} - 2) to a smaller, equivalent number. If after doing this reduction once, the result is more than 12 bits, do it a second time to reduce it further.
3. Below is Horner's method of polynomial evaluation with four different variations. For each variation determine the equivalent polynomial. Write "..." to indicate "the pattern continues until", and use x_i instead of x[i]. Hint: The first one is $x_0\ k^n + x_1\ k^{n-1} + \ldots + x_{n-1}\ k$.

```
res = 0
for (i=0; i<n; i++)
    res = res + x[i]
    res = res * k
```

```
res = 0
for (i=0; i<n; i++)
    res = res * k
    res = res + x[i]
```

```
res = 1
for (i=0; i<n; i++)
    res = res + x[i]
    res = res * k
```

```
res = 1
for (i=0; i<n; i++)
    res = res * k
    res = res + x[i]
```

4. Recall that H is ε-almost-universal if the probability h(a)=h(b) is no more than ε when a ≠ b and h ∈ H is chosen randomly. The following H is a family of functions all with domain Z_6 and co-domain Z_4. For what value of ε is H ε-almost-universal? Show your work by listing all probabilities calculated. H is defined as follows:

```
     h1  h2  h3  h4  h5
---+----------------------
 0 | 2   3   0   1   3
 1 | 3   2   1   0   0
 2 | 0   1   3   2   1
 3 | 0   0   2   2   3
 4 | 2   1   1   3   2
 5 | 0   3   3   2   0
```

5. Let's say you are using a polynomial hash function $k^{n+1} + x_0\, k^n + x_1\, k^{n-1} + \ldots + x_{n-1}\, k \bmod p$ to hash the three-byte data `0x 26 14 04`, and let's say that p=257, k is randomly chosen to be 0x55, and that the data is broken into 8-bit chunks before hashing. What is the resulting value?
6. Can you find another data string (of any length) that yields the same output value?
7. We saw that an authentication tag can be generated by combining a universal hash like the one above with a random function: TagGen(x, n) = h(x) op f(n). (The operation used depends on the specifics of h and f.) Because it's readily available, let's say we are using the AES S-box for f, the hash function listed above with k=0x55 for h, and addition mod p=257 for the TagGen operation. What authentication tag is generated for the three-byte data `0x 26 14 04` when the nonce used is 0x10?
8. *Cryptography Engineering* Exercises 5.5 and 6.2.

Ungraded homework solutions

These are best studied after completing the homework or after struggling with it for a while.

Solutions PDF.