Problem Set 2

Christopher Seaman

2007-10-03

The work on this problem set is my own. Ben Baumer and I consulted on problem 4.

1

Given $x_0 = 1$, $x_1 = 4$, $x_2 = 9$, and knowing that $x_{i+1} = A \cdot x_i + B$ we get the following equations:

$$4 \equiv 1 \cdot A + B \mod 65537$$

$$9 \equiv 4 \cdot A + B \mod 65537$$

Which implies that

$$5 \equiv 3 \cdot A$$

So we just have to find $3^{-1} \mod 65537$ to find A. By the magical matrix reduction method (linear algebra form of the extended euclidean algorithm):

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 65537 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 3 \\ -21845 & 1 & 2 \end{pmatrix} \Rightarrow \begin{pmatrix} 21846 & -1 & 1 \\ -21845 & 1 & 2 \end{pmatrix}$$

Which gives us $21846 \equiv 3^{-1} \mod 65537$. Returning to just before calculating 3^{-1}:

$$5 \equiv 3 \cdot A \mod 65537$$

$$21846 \cdot 5 \equiv 21846 \cdot 3 \cdot A \mod 65537$$

$$109230 \equiv 43693 \equiv A \mod 65537$$

Plugging in to the original congruences gives us:

$$4 \equiv 43694 + B \mod 65537$$

$$B \equiv 21848 \mod 65537$$

And test it out:

$$4 \cdot 43693 + 21848 = 196620 \equiv 9 \mod 65537$$

Okay, so what is the next number?

$$9 \cdot 43693 + 21848 = 415085 \equiv 21863$$

2

2.1

$| x |= 3$ which means that p is odd and at least 7 (as $\mod 5$ there are no elements of order 3). Also, 3 divides $(p-1) = \phi(p)$.

$$(x+1)^k = \sum_{i=0..k} \binom{k}{i} x^i$$

I think that this will only be congruent to 1 when x^k is congruent to the identity, so the order of $(x+1)$ is a multiple of 3.

Trying a different tactic, I've noticed that $(x+1)^2 = x$ in all the groups I've tried, maybe that holds for all x

$$(x+1)^2 = x^2 + 2x + 1 \Rightarrow x(x+1)^2 = x^3 + 2x^2 + x$$
$$x(x+1)^2 = 2x^2 + x + 1$$
$$x(x+1)^2 = x^2 + 2x + 1 + x^2 - x$$
$$x(x+1)^2 = (x+1)^2 + x(x-1)$$
$$x(x+1)^2 - (x+1)^2 = x(x-1)$$
$$(x-1)(x+1)^2 = x(x-1)$$
$$(x+1)^2 = x$$

So this gives us $1 \equiv x^3 \equiv ((x+1)^2)^3$. Noting that $(x+1)$ squared and cubed cannot be congruent to 1, the order of $(x+1)$ must then be 6.

2.2

So 2 and 3 generate the group, so $|2| = |3| = p-1$. Suppose 6 did as well, then $|6| = p-1$ and $6^k \not\equiv 1, \forall k < (p-1)$.

$$6^k = 2^k \cdot 3^k \not\equiv 1 \mod p$$

There exists some $m < (p-1)$ such that $2^m = 3$.

$$2^k \cdot 2^{mk} \not\equiv 1 \mod p$$

Let $z = mk \mod \phi(p)$, noting that $z \neq k$ as $2 \neq 3$, $z > 0$ because $2^{mk} = 3^k \not\equiv 1$, and $z < (p-1)$.

$$2^k \cdot 2^z \not\equiv 1 \mod p$$

$$2^{k+z} \cdot 2^{-z} \cdot 2^z \not\equiv 1 \mod p$$

$$2^{k+z} \not\equiv 1 \mod p$$

But, you say, letting $k = p-1-z$ gives $2^{k+z} \equiv 2^{p-1} \equiv 1 \mod p$. This contradicts $6^k \not\equiv 1$ for $k < (p-1)$, so 6 is not primitive.

3

First, we know that vowels must be more common than consonants as each consonant must be followed by at least one vowel. To check quickly if a string of letters could be valid Hawaiian we need only check that each consonant is followed by a vowel. If there is ever a fault then the message is definitely not Hawaiian. If the string validates then we are as confident in it being Hawaiian as we are that the string did not occur by chance.

We're dealing with compound probability here, the probability of having true Hawaiian for a given number of consonants and the probability of getting enough consonants to be able to tell if we have true Hawaiian.

If we take a conservative stance that a vowel is only 50% likely, then we need to check the letters after 6 consonants to get $p = (1/2^6) = 0.015625 < 0.025$ to be more than 97.5% confident that our string is actually Hawaiian. At the bare minimum this requires 12 letters. To estimate the string length necessary to be 95% sure we get 6 consonants, conservatively estimate the density of consonants at 20%. Using the binomial expansion where N = total letters, x = number of consonants, and $p = 0.2$ the probability of getting a consonant:

$$\frac{N!}{x!(N-x)!}p^x(1-p)^{N-x}$$

Using a quick script to find the sum of the probabilities of getting 5, 6, 7, ... , N consonants for increasing string lengths I received my answer. Given the probabilities above, a string of length 55 has $p > 0.975$ of containing at least 6 consonants. Since we need to guarantee a letter after each consonant, we'll take a string of length 56. The script was:

```
sub factorial {
  my ($n) = @_;
  if ($n < 2) {return $n;}
  else {return $n * fac($n-1);}
}

my $p = 0;
my $n = 6;
while($p < 0.975){
$p = 0;
for (my $x = 6; $x <= $n; $x++){
$p = $p + ((&factorial($n))/((&factorial($x))*(&factorial($n-$x)))*((0.2)**($x))*((0.8)**($n-$x)));
}
print "N = $n\tp = $p\n";
$n++;
}
```

We know that valid strings with 6 consonants are $p > .975$ of being Hawaiian and valid strings of more consonants have even higher p, so let's set the lower bound of this probability at $p_{hawaiian} = 0.975$. The probability of getting enough consonants (given a string of length 55 plus an additional letter) is $p_{letters} = 0.975$, so $p_{hawaiian} \cdot p_{letters} > 0.95$ giving us 95% confidence that a valid string of length 56 is really Hawaiian.

Additionally, this algorithm should be fairly efficient to implement as it really only requires shifts and lookups.

4

4.1

If we take $n = 103pq$ then $\phi(n) = 102pq = (2)(3)(17)pq$. Against an attack attempting to factor n, multiplying by n by 103 doesn't make factoring n any easier. Changing n makes for 102 sets of the original keyspace.

As for whether the RSA algorithm will still function, that is up in the air. For e of binary weight two, it is possible that $e \in \{3, 17\}$. Unfortunately, 3 and 17 are also divisors of $\phi(n) = \phi(103pq) = (2)(3)(17)pq$. This implies that the gcd $(e, \phi(n)) > 1$, so there may not exist a d such that $ed \equiv 1 \mod \phi(n)$. Not having d breaks decryption, which is generally considered an essential part of RSA.

4.2

As above, if $(e, \phi(n)) > 1$ then we no longer have a d and cannot decrypt our ciphertext.