Cryptography 2/7

Reagan Shirk

February 7, 2020

Repeating Squaring Algorithm

- First algorithm:
  - Simple but effective
  - Time complexity: $O(log(b)log^2(n))$
    - I think he said this is a pessimistic time complexity?
    - We don't really care about the second half of the complexity
  - Good algorithm
  - You can remove the last if statement and have the final return take its place

```
modpower(a, b, n)
# compute a**b mod n
# assume a, n position integer, b non negative integer
    if b == 0:
        return 1
    if b is even:
        return modpower(a**2 % n, b/2, n)
    if b is odd:
        return a * modpower(a, b - 1, n)  % n
```

- Second Algorithm
  - Assumbe $b = b_k b_{k-1} \cdots b_1$ and $b_k = 1$
  - Better than the above algorithm when the base = 2

```
# compute base**b mod n
result = base
for i in range(k - 1, 0, -1):
    result == result**2 % n
    if b_i == 1:
        result = result * base % n
```

- Lets look at base^{1010}
  - This means you're calculating base$^{2^3}$ $\times$ base$^{2^2}$ for the first algorithm
    - You have three squares and one multiplication with the base
  - This means you're calculating $((\text{base}^2)^2\text{base})^2$ for the second algorithm
    - You have three squares and one multiplication with the base

Chinese Remainder Theorem

- Suppose you have a 6 digit passcode, and one day your "friend" asks you for the remainder when you divide your passcode by 2 (i.e. is it even or odd?) - you answer and reveal the last bit of information
  - The "friend" asks again for the remainder by 3, and the next day asks for the remainder by 5
  - "Basically the chinese remainder theorem tells you don't do that okay"
  - You can get a passcode by dividing by $2, 3, 5, 7, 11$ I think is what he said?
    - Ohhhh just prime numbers in general
- You have:

$$
\begin{aligned}
a &\equiv b_1 \bmod 2 \\
a &\equiv b_2 \bmod 3 \\
&\vdots \\
a &\equiv b_n \bmod p_n
\end{aligned}
$$

- It's called the chinese remainder theorem because it was created by a chinese general (General Sun)
  - Not sure if this is legitimate or if it was a set up for a joke but it was a good story that I'll write out later if I remember