Cryptography Notes

Richard Awojoodu

February 23, 2017

Modular Exponentation: The idea is to take our exponent and compute $a^n(mod m)$ very quickly

Modular Exponentation Steps:

1. Write out exponent in Binary Form!
2. Use repeated squaring to compute each power of 'a' to an exponent that is a multiple of 2; reduce modulo 'n' after EVERY square.
3. Using the table from repeatd squaring, multiply together the binary expansion terms!

Examples: Compute $3^{521}(mod 19)$ using the method of repeated squaring!
We know that 521 = 512 + 8 + 1.
521(base2) = 1000001001

1. $3^1 = 3(mod 19)$
2. $3^2 = 9(mod 19)$
3. $3^4 = 5(mod 19)$
4. $3^8 = 6(mod 19)$
5. $3^{16} = 17(mod 19)$
6. $3^{32} = 4(mod 19)$
7. $3^{64} = 16(mod 19)$
8. $3^{128} = 9(mod 19)$
9. $3^{256} = 5(mod 19)$
10. $3^{512} = 6(mod 19)$

    Therefore,$3^{521} = 3^{512} + 3^8 + 3^3(mod 19)$ = 6 + 6 + 3(mod19)=13$(mod 19)$

Fermat's (Little) Theorem: The idea is that "If 'P' is a prime number and 'a' is not divisible by 'P' then $a^{p-1} = 1(mod p)$

Examples:

1. P = 5 , a = 2 , $2^{5-1} = 16 = 3(5) + 1$ WORKS!
2. P = 7, a=2 , $2^(7-1) = 64 = 9(7) + 1$ WORKS!
3. P = 5, a=3 , $3^(5-1) == 81 = 16(5) + 1$ WORKS!

Proof: Let S = 1,2,3,.....,P-1 all the non-zero residues mod p
The Set $f_a(1), f_a(2), f_a(3), ..., f_a(p-1) = S$
= $f_a(1) * f_a(2) * f_a(3) * .... * f_a(p-1)(mod p)$
=$1 * 2 * 3 * .... * (p-1)(mod p))$
=$a(1) * a(2) * a(3) * .... * a(p-1)(mod p)$
Then, $(p-1)! = a^{p-1}(mod p)$
Finally, $1 = a^{p-1}(mod p)$

Example: Compute $3^{602}(mod 101)$

1. 101 is Prime, so $3^{100} = 1(mod 101)$
2. =$3^{6*100+2}(mod 101)$
3. =$(3^{100})^6 * 3^2(mod 101)$
4. =$1 * 9(mod 101)$