Foundation of Cryptography

Session 21

Date: 19 March 2021

Dr. V. K. Pachghare

Chinese Remainder Theorem

Find a solution using Chinese remainder theorem to $p^2 = 1 \pmod{144}$

$144 = 16 \times 9 = 2^4 \times 3^2$

GCD (16, 9) = 1

Therefore,

$P^2 = 1 \bmod 16$ having 4 solutions (2^4 here power is 4)

$P = \pm 1$ or $\pm 7 \bmod 16$ ($b_1 \Rightarrow \pm1, \pm 7$)

$P^2 = 1 \bmod 9$ having 2 solutions (3^2 here power is 2)

$P = \pm1 \bmod 9$ ($b_1 \Rightarrow \pm1$)

Obtaining $b_i = \pm1, \pm7$.

$p = 1 \pmod{16}$	$p = 1 \pmod{9}$
$p = 1 \pmod{16}$	$p = -1 \pmod{9}$
$p = -1 \pmod{16}$	$p = 1 \pmod{9}$
$p = -1 \pmod{16}$	$p = -1 \pmod{9}$
$p = 7 \pmod{16}$	$p = 1 \pmod{9}$
$p = 7 \pmod{16}$	$p = -1 \pmod{9}$
$p = -7 \pmod{16}$	$p = 1 \pmod{9}$
$p = -7 \pmod{16}$	$p = -1 \pmod{9}$

Here $n_1 = 16$, $n_2 = 9$

Each case has unique solution for x mod 144

$b_1 = \pm 1, \pm 7$

$N = n_1 * n_2$

$= 16 \times 9$

$= 144$

and find the value of $N_i = N/n_i$ as below:

$N_1 = 144/16 = \mathbf{9}$

$N_2 = 144/9 = \mathbf{16}$

Now find out the multiplicative inverse as below:

$y_i \equiv (N_i)^{-1} \pmod{n_i}$

$y_1 = (9)^{-1} \pmod{16} \quad = 9$

$y_2 = (16)^{-1} \pmod{9} \quad = 4$

The solution for above problem is:

$P \equiv [b_1N_1y_1 + b_2N_2y_2] \bmod N$

$b_i = \pm 1, \pm 7$

$N_1 = 9, \quad N_2 = 16$

$y_1 = 9, \quad y_2 = 4$

$$\begin{aligned} p &= 1(9)(9) + 1(4)(11) \bmod 144 \\ &= 81 + 64 \\ &= 145 \bmod 144 \\ &= 1 \bmod 70 \end{aligned}$$

So the solution is 1

p = 1(9)(9) + (-1)(4)(16) mod 144
= 81 - 64
= 17 mod 144
So the solution is 17

p = -1(9)(9) + (1)(4)(16) mod 144
= -81 + 64
= -17 mod 144
So the solution is -17

p = (-1)(9)(9) + (-1)(4)(16) mod 144
= -81 - 64
= -145 mod 144
So the solution is -1

p = (7)(9)(9) + (1)(4)(16) mod 144
= 567 + 64
= 631 mod 144 = 55 mod 144
So the solution is 55

p = (7)(9)(9) + (-1)(4)(16) mod 144
= 567 - 64
= 503 mod 144 = 71 mod 144
So the solution is 71

p = (-7)(9)(9) + (1)(4)(16) mod 144
= -567 + 64
= -503 mod 144 = -71 mod 144
So the solution is -71

p = (-7)(9)(9) + (-1)(4)(16) mod 144
= -567 - 64
= -603 mod 144 = -55 mod 144
So the solution is -55

P = 1, 17, -17, -1, 55, 71, -71, -55