Silver-Pohilg Hellman Algorithm Implemented To Discrete Log With Arya Bhatta Remainder Theorem

Surendra Talari, Department of Mathematics, GIS, GITAM Deemed to be University, Visakhapatnam, AP, India

P. Sirisha, Indian Maritime University, Visakhapatnam, AP, India

D. Sateesh Kumar, Department of Mathematics, Konerulakshmaiah Education Foundation, Vaddeswaram, Guntur, AP, India

K.L. Sowmya, Department of Computer Science, GIT, GITAM Deemed to be University, Visakhapatnam, AP, India

K. Divakara Rao, Indian Maritime University, Visakhapatnam, AP, India

Abstract---As the internet provides access to millions of communications in every second around the world, security implications are tremendously increasing. Transfer of important files like banking transactions, tenders, and e commerce require special security and authenticated mechanism in its journey from the sender to the receiver. Public key Cryptosystem (PKC) is ever expanding in the history of cryptography. Traditional Public Key Infrastructure (PKI) certificates assure the authenticity in the form of digital signature. Public key cryptosystem having wide range of practical applications in wireless environments like smartcards, tokens and mobile phones. In this paper we solved discrete log problems with Silver Pohilg Hellman algorithm Implemented to Discrete Log with Aryabhatta Remainder Theorem, which improves the difficult of solving discrete log. So obviously it improves the security of public key crypto systems and avoids various attacks on it.

Key words---Discrete log, Chinese Reminder Theorem, Aryabhatta Remainder Theorem (ART), finite field.

Introduction

Public key Cryptosystem (PKC) is ever expanding in the history of cryptography. Public key cryptosystem [**12,20**] having wide range of practical applications in wireless environments like smartcards, tokens and mobile phones. The Discrete Logarithm Problem (DLP) and the Elliptic Curve Discrete Logarithm Problem (ECDLP), along with the Integer Factorization Problem (IFP), are the three most important infeasible computational problems in computational number theory and modern cryptography. The difficulty of solving discrete log problem plays a major role in the security of public key crypto systems, so if the finding the solution of discrete log is difficult the public key crypto system [**10,11,15**] is more secure. [**21**] The Russian mathematician Bouniakowsky [**16**] developed a clever algorithm to solve the congruence ax ≡b (mod n), with the asymptotic complexity O(n) in 1870. Despite its long history, no efficient algorithm has ever emerged for the Discrete Logarithm Problem. [**1,9,14**] In this paper we solved discrete log problems with Silver-Pohilg Hellman algorithm implemented with Aryabhatta Remainder Theorem, which improves the difficult of solving discrete log. The decryption speed can be improved by reducing the number of modulo inverse operations required to solve the congruence. Aryabhatta Remainder Theorem takes only one modulo inverse operation to solve two congruence relations. When compared with Chinese Remainder Theorem, ART requires lesser modulo inverses. [**17**] Also we applied programming concepts for the proposed method in c language, so the implementations will be easy and can solve for large values. We made number of trails in executing the proposed algorithm for various problems with different large primes and found that the execution time is varies. Where as if we implement with existing methods for the same problems and with the same prime numbers [**7**] we found that the execution time is almost similar. Since with the proposed method the execution time of the problems is varies it avoids the attacks [**18, 19**] like time attack or side channel attack on the cryptosystem.

Literature

In1978, Pohligand Hellman [**16**] proposed an important special algorithm, now widely known as the Silver–Pohlig–Hellman algorithm for computing discrete logarithms [**10,11,15**] over GF(q) with O(√p) operations and a comparable amount of storage, where p is the largest prime factor of q −1.

DOI: 10.5373/JARDCS/V12I2/S20201354
* *Corresponding Author: Surendra Talari, Email:surendrat.bw@gmail.com*
Article History: Received: Mar 22, 2020, Accepted: June 24, 2020

2.1 Silver-Pohlig-Hellman Algorithm for finding discrete logs in finite [3,4,5]:

Let F_q be the finite field, for q being a prime power such that q-1 has all small prime factor (i.e., q-1 is smooth). Also let b be a generator of F_q^* and for any y ϵF_q^*,the discrete log of y to the base 'b' is computed as follows.

For each prime p/q-1, define the p^{th} root of unity $r_{p,j} = b^{(q-1)j/p}$, $0 \le j < p$ and consider the set $\{r_{p,j}\}_{0 \le j < p}$ now to find x ∋ $0 \le x < q-1$ with $y=b^x$, it is enough to compute $x \pmod{p^\alpha}$ for $q-1 = \pi_{p/q-1} p^\alpha$ as the uniqueness of x is determined by Chinese-remainder theorem.

Any x mod p^α may be written as $x \equiv x_0+x_1p+x_2p^2+\ldots+x_{\alpha-1}p^{\alpha-1} \pmod{p^\alpha}$ for some $0 \le x_i < p \ \forall\ i=1,2,\ldots\alpha-1$; To find x mod p^α, we need to find all x_i. Now to find x_0, we compute $y^{q-1/p}$,

$y^{q-1/p} = b^{x(q-1)/p}$

$= b^{(x_0+x_1p+x_2p^2+\cdots x_{\alpha-1}p^{\alpha-1}+p^\alpha.t_c)q-1/p}$ for some $t_0 \in z$

$= b^{x_0(q-1)/p} \cdot b^{(q-1)t_0'}$, for some $t_0' \in z$

$= b^{x_0(q-1)/p}$ [$\because b^{(q-1)} = e$]

$= r_{p_1x_0}$.Since $y^{q-1/p}$ is a p-th root of unity $\Rightarrow y^{q-1/p} \in \{r_{p,j}\}$

$\Rightarrow y^{q-1/p} = r_{p,j}$ for some j

$\Rightarrow x_0 = j$.

To find x_1, we take $y_1 = \frac{y}{b^{x_0}} = b^{x-x_0}$ and compute, $y_1^{q-1/p^2} = b^{x-x_0(q-1)/p^2}$

$= b^{(x_1p+x_2p^2+\cdots x_{\alpha-1}p^{\alpha-1}+p^\alpha t_1)(q-1)/p^2}$

$= b^{x_1(q-1)/p} \cdot b^{(q-1)t_1'}$

$= b^{x_1(q-1)/p} = r_{p,x1}$

As $y_1 = b^{x-x_0} = b^{t'.p}$, p-th power &for some $t' \in z$. We have $y_1^{q-1/p} = \left(b^{t'.p}\right)^{\frac{q-1}{p}} = b^{t'.(q-1)} = 1$. Since y_1^{q-1/p^2} is a p-th root of unity, we have $y_1^{q-1/p^2} = r_{p,j}$ for some j and $x_1 = j$. We find x_i , by taking $y_i = \frac{y}{b^{x_0+x_1p+\cdots x_{i-1}p^{i-1}}}$ and compute $(y_i)^{\frac{q-1}{p^{i+1}}}$. By definition, we have $y_i^{q-1/p^{i+1}} = r_{p_1x_1}$ ……..(2) & also note $y_i = b^{p^i.t'}$, i.e., p^i-th power such that $(y_i)^{\frac{q-1}{p^i}} = 1$, therefore $(y_i)^{\frac{q-1}{p^{i+1}}} = r_{p,j}$ for some j. From equation (2) we have $x_i = j \ \forall\ i = 0,1,2,\ldots.\alpha-1$. Therefore by substituting for all x_i's in $x \equiv x_0 + x_1 p + \ldots + x_{\alpha-1}p^{\alpha-1} \pmod{p^\alpha}$, we get $x \pmod{p^\alpha}$. Now we solve above system of congruence's with Chinese remainder theorem [**3,4,5**].

2.2 Chinese Remainder theorem:[16]

Suppose that we want to solve a system of congruences to different modulo

$x \equiv a_1 \bmod m_1$,

$x \equiv a_2 \bmod m_2$,

……

$x \equiv a_r \bmod m_r$

Suppose that each pair of module is relatively prime: g.c.d$(m_i, m_j) = 1$ for $i \neq j$, then there exists a simultaneous solution x to all of the congruences and any two solutions are congruent to one another modulo $M = m_1m_2m_3\ldots.m_r$. That is the system of congruence has exactly one solution modulo the product $m_1m_2m_3\ldots.m_r = M$. [**6,8,13**]

Proof: First we prove uniqueness modulo M.

Suppose x^1 and x^{11} are two solutions and let $x = x^1 - x1.1$

Since $x^1 \equiv a_1 \bmod m_1$……..$x^1 \equiv a_r \bmod m_r$ and $x^{11} \equiv a_1 \bmod m_1, \ldots x^{11} \equiv a_r \bmod m_r$, then $x \equiv 0 \pmod{m_i}$ for each i. Which implies that $x \equiv 0 \pmod M$.

Since if $a \equiv b \pmod m$, $a \equiv b \pmod n$ and (m,n)=1 implies that $a \equiv b \pmod{m.n}$. So from the above relations we have $x^1 - x^{11} \equiv 0 \pmod M$ which implies that $x^1 \equiv x^{11} \pmod M$.

Therefore the system of congruence's has exactly one solution modulo M where $M = m_1.m_2.m_3\ldots\ldots m_r$.

Existence of solution: Define $M_i = M/m_i$, i=1,2,3…r, then $(M_i, m_i) = 1$. Since $(m_i, m_j) = 1$ for $i \neq j$ there is $N_i \in Z$. By Euclidean algorithm such that $M_iN_i \equiv 1 \pmod{m_i}$ for i=1,2,3…r $(1 = M_iN_i + cm_i)$.

Now let $x= \sum_{i=1}^{r} a_i M_i N_i$ and since $m_k / \sum_{i=1}^{r} a_i M_i N_i - a_k M_k N_k$ which implies $\sum_{i=1}^{r} a_i M_i N_i \equiv a_k M_k N_k \pmod{m_k}$. But $M_i N_i \equiv 1 \pmod{m_i}$ for i=1,2,…r which impiles that $M_k N_k \equiv 1 \pmod{m_k}$, that is $\sum_{i=1}^{r} a_i M_i N_i \equiv a_k \pmod{m_k}$. Hence $x \equiv a_k \pmod{m_k}$ and therefore x satisfies every congruence in the system.

3. Proposed Method

3.1 Silver-Pohlig-Hellman Algorithm extended to Aryabhatta Remainder Theorem (ART) [2]:

Let F_q be the finite field, for q being a prime power such that q-1 has all small prime factor (i.e., q-1 is smooth). Also let b be a generator of F_q^* and for any y ϵF_q^*,the discrete log of y to the base 'b' is computed as follows.

For each prime p/q-1, define the p^{th} root of unity $r_{p,j} = b^{(q-1)j/p}$, $0 \le j < p$ and consider the set $\{r_{p,j}\}_{0 \le j < p}$ now to find x ∋ $0 \le x < q-1$ with $y=b^x$, it is enough to compute $x \pmod{p^\alpha}$ for $q-1 = \pi_{p/q-1} p^\alpha$ as the uniqueness of x is determined by Chinese-remainder theorem.

Any x mod p^α may be written as $x \equiv x_0 + x_1 p + x_2 p^2 + \ldots + x_{\alpha-1} p^{\alpha-1} \pmod{p^\alpha}$ for some $0 \le x_i < p \; \forall$ i=1,2,…α-1; To find x mod p^α, we need to find all x_i. Now to find x_0, we compute $y^{q-1/p}$,

$y^{q-1/p} = b^{x(q-1)/p}$

$= b^{(x_0 + x_1 p + x_2 p^2 + \cdots x_{\alpha-1} p^{\alpha-1} + p^\alpha . t_c)q-1/p}$ for some $t_0 \in z$

$= b^{x_0 (q-1)/p} . b^{(q-1) t_0'}$, for some $t_0' \in z$

$= b^{x_0 (q-1)/p}$ [$\because b^{(q-1)} = e$]

$= r_{p_1 x_0}$. Since $y^{q-1/p}$ is a p-th root of unity $\Rightarrow y^{q-1/p} \in \{r_{p,j}\}$

$\Rightarrow y^{q-1/p} = r_{p,j}$ for some j

$\Rightarrow x_0 = j$.

To find x_1, we take $y_1 = \frac{y}{b^{x_0}} = b^{x-x_0}$ and compute, $y_1^{q-1/p^2} = b^{x - x_0 (q-1)/p^2}$

$= b^{(x_1 p + x_2 p^2 + \cdots x_{\alpha-1} p^{\alpha-1} + p^\alpha t_1)(q-1)/p^2}$

$= b^{x_1 (q-1)/p} . b^{(q-1) t_1'}$

$= b^{x_1 (q-1)/p} = r_{p,x1}$

As $y_1 = b^{x-x_0} = b^{t'.p}$, p-th power &for some $t' \in z$. We have $y_1^{q-1/p} = \left(b^{t'.p}\right)^{\frac{q-1}{p}} = b^{t'.(q-1)} = 1$. Since y_1^{q-1/p^2} is a p-th root of unity, we have $y_1^{q-1/p^2} = r_{p,j}$ for some j and $x_1 = j$. We find x_i , by taking $y_i = \frac{y}{b^{x_0 + x_1 p + \cdots x_{i-1} p^{i-1}}}$ and compute $(y_i)^{\frac{q-1}{p^{i+1}}}$. By definition, we have $y_i^{q-1/p^{i+1}} = r_{p_1 x_1}$ ……..(2) & also note $y_i = b^{p^i . t'}$, i.e., p^i-th power such that $(y_i)^{\frac{q-1}{p^i}} = 1$, therefore $(y_i)^{\frac{q-1}{p^{i+1}}} = r_{p,j}$ for some j. From equation (2) we have $x_i = j \;\; \forall$ i = 0,1,2,….α-1. Therefore by substituting for all x_i's in $x \equiv x_0 + x_1 p + \ldots + x_{\alpha-1} p^{\alpha-1} \pmod{p^\alpha}$, we get x (mod p^α). Now we solve above system of congruence's with following Aryabhatta Remainder Theorem (ART).

3.2 ART algorithm for two residues:

If $x \equiv x_1 \pmod{p_1}$, $x \equiv x_2 \pmod{p_2}$ and $(p_1,p_2)=1$ then it has only one solution in Z_P where $P = p_1 p_2$. The solutions is

$x = ART(q_1,q_2; p_1,p_2;P)$

$x = ART(0,|q_2-q_1|_p; p_1p_2)+q_1$

$x = A + q_1$ where $A = p_1[(c.p_1^{-1}) \bmod p_2$ where $c = q_2-q_1$.

3.3 ART algorithm for more residues [2,17]:

$x \equiv x_1 \pmod{p_1}$, $x \equiv x_2 \pmod{p_2}$… $x \equiv x_t \pmod{p_t}$ and $(P_I,P_J)=1$ for $I \ne J$ where I=J=1,2,…t, then it has only one solution in Z_P where $P = p_1 p_2 \ldots p_t$.

The solutions is

$x = ART(q_1,q_2,q_3 \ldots . q_t; p_1,p_2 \ldots . p_t;P)$ where $P = p_1 . p_2 \ldots . p_t$

Step 1: $x_1 = q_1$

Step 2: $x_2 = ART(q_1,q_2; p_1,p_2;P_2)$ where $P_2 = p_1 . p_2$

$x_2 = ART(0, |q_2 - q_1|_{mod\ p_2}; p_1,p_2;P_2)+q_1$

Step 3: $x_3 = ART(x_2,q_3; p_2,p_3;P_3)$ where $P_3 = p_1 . p_2 . p_3$

$x_3 = ART(0, |q_3 - x_2|_{mod\ p_3}; p_2,p_3;P_3)+q_2$

Step 3: $x_t = ART(x_{t-1},q_t; p_{t-1},p_t;P_t)$ where $P_t = p_1 . p_2 . p_3 \ldots p_t$

DOI: 10.5373/JARDCS/V12I2/S20201354

* *Corresponding Author: Surendra Talari, Email:surendrat.bw@gmail.com*

Article History: Received: Mar 22, 2020, Accepted: June 24, 2020

$X_t = ART(0, |q_t - x_{t-1}|_t; p_{t-1}, p_t; P_{t-1}) + q_t$

3.4 Algorithm :

To solve discrete log problem of y to the base b over the finite field F_q using Silver-Pohlig-Hellman Algorithm extended to Aryabhatta Remainder Theorem (ART)

Step 1: Input the values of q,b,y

Step 2: Find prime divisors of q-1 of the form $p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots . p_n^{\alpha_n}$

Step 3:Write $x \equiv x_0+x_1p+x_2p^2+\ldots+x_{\alpha-1}\, p^{\alpha-1} \pmod{p^\alpha}$ for some $0 \le x_i < p \ \forall\ i=1,2,\ldots\alpha-1$

Step 4: Find all xi for i= i=1,2,…α-1 for all pj where j=1,2,..n

Step 5: write congruence relations with xi in step 4 for each pj where j=1,2,..n

Step 6: Solve step 5 congruence relations with ART

Step 7: We get the solution of discrete log

3.5 Implementation 1:

We solved the discrete log 153 to the base 2 in F_{181}^* (2 is a generator of F_{181}) using the Silver-Pohilg Hellman algorithm extended to Aryabhatta Remainder Theorem (ART) [**16**]. Since the prime number value q=181, b=2 & y=153, the prime divisors of q-1=180 are 2,3 and 5, since $180=2^2 *3^2 *5$. The p-th root of unity is $r_{p,j} = b^{j(q-1)/p}$, $0 \le j < p$, for p=2 , $r_{2,j} = \{r_{2,0}, r_{2,1}\}$ where $r_{2,0}=1$ and $r_{2,1}= 2^{90} \pmod{181}=180$. Therefore $r_{2,j}=\{1,180\}$ in modulo q, now for $x \equiv x_0+x_1p+\ldots+x_{\alpha-1}\, p^{\alpha-1} \pmod{p^\alpha}$, for for p=2 , we have $\alpha=2 \Rightarrow x \equiv x_0+x_1p \pmod 4$ implies $x \equiv x_0+2x_1 \pmod 4$. To compute x, we need to compute x_0 & x_1, further to find x_0, first we have to find $y^{q-1/p} \pmod q = 180$ which is equal to $r_{2,x0}$. Since $y^{q-1/p}$ is a p-th root of unity also $y^{q-1/p} \in \{r_{p,j}\}_{0 \le j < p}$ implies $r_{2,x0} = r_{2,1}$ hence therefore $x_0 = 1$. Now taking $y_1 = \frac{y}{b^{x_0}} \pmod q = 167$ and to find x_1 further have to find $y_1^{q-1/p^2} (mod\ q)=180= r_{2,x_1}$. Since $y_1^{q-1/p^2} \in \{r_{2,j}\}_{0 \le j < 2}$ hence implies $r_{2,x_1} = r_{2,1}$ and therefore $x_1=1$. Now substituting x_0 & x_1 values in $x \equiv x_0+x_1p \pmod{p_1}$we get**$x \equiv 3 \rightarrow$(a)** for the prime p_1. Repeating the above argument for **p=3 and α=2** we have $r_{3,j}=\{r_{3,0},r_{3,1},r_{3,2}\} \pmod q = \{1,48,132\}$ & $x \equiv x_0 + 3x_1 \pmod 9$. To find x_0 we have to find $y^{q-1/p} \pmod q = 132 = r_{3,x_0}$. Since $y^{q-1/p} \in \{r_{3,j}\}_{0 \le j < 3}$ implies $r_{3,x_0} = r_{3,2}$ hence $x_0 = 2$. Now taking the expression $y_1 = \frac{y}{b^{x_0}} (mod\ q)=174$. To find x_1 we have to find $y_1^{q-1/p\wedge 2} \pmod q = 132 = r_{3,x_1}$ which implies $r_{3,x1} = r_{3,2}$ hence we get $x_1 =2$. Therefore **$x \equiv 8 \pmod 9 \rightarrow$(b)** for the prime p_2**.**

Again for **p=5 & α=1** and $x \equiv x_0 \pmod 5$ also $r_{5,j} = \{ r_{5,0}, r_{5,1}, r_{5,2}, r_{5,3}, r_{5,4}\}=\{1,59,42, 125,135\}$. To find x_0 we have t calculate $y^{q-1/p} \pmod q = 42 = r_{5,x0}$ and hence we get $x_0 = 2$. Therefore **$x \equiv 2 \pmod 5 \rightarrow$(c)** for the prime p_3**.**

Now solving equations (a), (b) & (c) by Aryabhatta Remainder Theorem [**2**] we have $p_1 =2^2$, $p_2 = 5$ & $p_3 =3^2$and $P =2^2.5.3^2=180$.

Here $q_1=3$, $q_2 =8$ & $q_3=2$;

x = ART (3,8,2;4,5,9;180)

Step 1: $x_1=3$

Step 2: x_2 = ART(3,8; 4,5;20)

$x_2 = ART(0, |1-3|_{mod\ 5}; 4,5;20)+3$

x_2 =ART(0,3; 4,5;20)+3

$x_2 = A+3$ where $A= p_1[(c.p_1^{-1}) \bmod p_2]=35$

Step 2: x_3 = ART(35,9; 9,2;18)

$x_3 = ART(0, |35-9|_{mod\ 9}; 9,2;18)+35$

x_3 =ART(0,8; 9,2;18)+35

$x_3 = 9(8.9^{-1} \pmod 9))+35$

$x_3 = 72+35=107$.

Therefore thesolution of thediscrete log 153 to the base 2 in $F_{181}^*$is 107.

3.6 Implementation 2:

We solved the discrete log 15 to the base 2 in F_{29}^* (2 is a generator of F_{29}) using the Silver-Pohilg Hellman algorithm extended to Aryabhatta Remainder Theorem (ART) [**17**]. Since the prime number value q=29, b=2 & y=15, the prime divisors of q-1=28 are 2 and 7. Since $28=2^2*7$, the p-th root of unity is $r_{p,j} = b^{j(q-1)/p}$, $0 \le j < p$, **for p=2** , $r_{2,j} = \{r_{2,0}, r_{2,1}\}$--- where $r_{2,0}=1$ and $r_{2,1}= 2^{14} \pmod{29}=28$. Therefore $r_{2,j}=\{1,28\}$ in modulo q, now for $x \equiv x_0+x_1p+\ldots+x_{\alpha-1}\, p^{\alpha-1} \pmod{p^\alpha}$, for for p=2 , we have $\alpha=2 \Rightarrow x \equiv x_0+x_1p \pmod 4$ implies $x \equiv x_0+2x_1 \pmod 4$. To compute x, we need to compute x_0 & x_1, further to find x_0, first we have to find $y^{q-1/p} \pmod q = 28$ which is equal to $r_{2,x0}$. Since $y^{q-1/p}$ is a p-th root of unity also $y^{q-1/p} \in \{r_{p,j}\}_{0 \le j < p}$ implies $r_{2,x0} = r_{2,1}$ hence therefore $x_0 = 1$. Now taking $y_1 = \frac{y}{b^{x_0}} \pmod q = 22$ and to find x_1 further have to find $y_1^{q-1/p^2} (mod\ q)=28= r_{2,x_1}$. Since $y_1^{q-1/p^2} \in \{r_{2,j}\}_{0 \le j < 2}$ hence implies $r_{2,x_1} = r_{2,1}$ and therefore $x_1=1$. Now substituting x_0 & x_1 values in $x \equiv x_0+x_1p \pmod{p_1}$we get**$x=3 \rightarrow$ (a)** for

the prime p_1. Repeating the above argument for **p=7 and α=1** we have $r_{7,j} = \{ r_{7,0}, r_{7,1}, r_{7,2}, r_{7,3}, r_{7,4}, r_{7,5}, r_{7,6} \} = \{$ (mod q) = {1,16,3,7,25,23,20} & $x \equiv x_0 \pmod 7$. To find x_0 we have to find $y^{q-1/p} \pmod q = 20 = r_{7,x_0}$. Since $y^{q-1/p} \in \{r_{3,j}\}_{0 \le j < 3}$ implies $r_{7,x_0} = r_{7,6}$ hence $x_0 = 6$. Therefore **$x \equiv 6 \pmod 7 \rightarrow$(b)** for the prime p_2**.**

Now solving equations (a) & (b) by Aryabhatta Remainder Theorem we have $p_1 = 2^2$ & $p_2 = 7$and $P = 2^2.7 = 28$.

Here $q_1 = 3$ & $q_2 = 6$

x = ART(3,6;4,7;28)

Step 1: $x_1 = 3$

Step 2: x_2 = ART(3,6;4,7;28)

x_2 = ART(0,$|6-3|_{\text{mod } 7}$; 6,7;28)+3

x_2 = ART(0,3; 6,7;28)+3

$x_2 = 27$

Therefore thesolution of thediscrete log 15 to the base 2 in F_{29}^* is 27.

Conclusion

As Public key cryptosystem [**12,20**] having wide range of practical applications in wireless environments like smartcards, tokens and mobile phones and also security of many public key cryptosystems based on difficulty of solving discrete log problems. In paper we solved discrete log problems using Silver-Pohilg Hellman algorithm Implemented to Discrete Log with Aryabhatta Remainder Theorem, which improves the difficult of solving discrete log. So obviously it improves the security [**21**] of public key crypto systems and avoids various attacks like pollard rho attack [**18, 19**] etc on it. The algorithm Silver-Pohilg Hellman for solving discrete log can be implemented with Chinese remainder theorem. The advantage of implementing above mentioned algorithm with ART is execution time. The running time is very less when implementing the algorithm for solving discrete log problem, which varies with earlier existing methods. So it avoids the side channel attack on the public key crypto systems. We can extend the implementation of ART in other algorithms which will use for solving discrete log problems. Also we implemented the above mentioned algorithm extended to ART by using programming concepts.

Acknowledgements

The authors would like to express their gratitude for the support offered by the Department of Mathematics, GIS, and GITAM Deemed to be University.

References:

[1] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, “Hand book of Applied Cryptography." CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[2] Chung-Huang Yang and Rao, T.R.N., Arabhata Remainder Theorem: Relevance to Public- Key Crypto-Algorithms, Circuits Systems Signal processing, Birkh¨a user Boston, Vol. 25, No. 1, PP. 1–15, 2006.

[3] Douglas R. Stinson “Cryptography theory and practice” Second edition.

[4] Gerhard Frey “The arithmetic behind cryptography” AMS volume 57, Number 3.

[5] Hans Delfs Helmut Knebl “Introduction to cryptography” Principles and its Applications, second edition.

[6] Harry Yosh “The key exchange cryptosystem used with higher order Diophantine equations” IJNSA VOL.3, 15. No.2, March 2011.

[7] I. Niven, H.S. Zuckerman and J.H. Silverman “An Introduction to the Theory of Numbers”, 5th ed., John Wiley and Sons, New York, 1991.

[8] J. Buchmann “Introduction to cryptography”, Springer Verlag 2001.

[9] Keith M. Martin, Rei Safavi-Naini, Huaxiong Wang and Peter R.Wild “Distributing the encryption and decryption of a block cipher”.

[10] Menzes A. and Vanstone S. “Hand book of applied cryptography”, The CRC-Press series of Discrete Mathematics and its Applications CRC-Press, 1997.

[11] Neal Koblitz “A course in number theory and cryptography” ISBN 3-578071-8, SPIN10893308.

[12] Peter J. Smith and Michael J.J. Lennon, “A New Public Key System” LUC Partners, Auckland UniServices Ltd, The University of Auckland, Private Bag92019m Auckland, New Zealand.

[13] Phillip Rogaway Mihir Bellare John Black Ted Krovetz “OCB: A block-cipher mode of operation for efficient authenticated encryption”.

DOI: 10.5373/JARDCS/V12I2/S20201354

* *Corresponding Author: Surendra Talari, Email:surendrat.bw@gmail.com*

Article History: Received: Mar 22, 2020, Accepted: June 24, 2020

[14] P.Rogaway, M-Bellare, J. Black,T-Korvetz "A Block Cipher mode of operation for efficient authenticated encryption" Eighth ACM conference on computer and communication security (CCS-8) ACM Press, 2001.
[15] Serge Vaudenay "A classical introduction to cryptography applications for communication security" Springer International Edition.
[16] [Song Y. Yan, "Number Theory for computing", 2nd edition, Springer, ISBN: 3-540-43072-5.
[17] Srinivas, B. and Bhagavan, V. S., On the usage of Aryabhatta Remainder Theorem for Improved performance on RP prime RSA, 2018. https://www.semanticscholar.org/paper/ON-THE-USAGE-OF-ARYABHATTA-REMAINDER-THEOREM-FOR-OF-Srinivas-Bhagavan/99abc10256b7c5d742ee2925865ce8 83f67a0660.
[18] Surendra Talari & P. Anuradha Kameswari, Pollard RHO algorithm implemented to Discrete Log with Lucas sequences, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume: 4, Issue: 3.
[19] Surendra Talari, P. Anuradha Kameswari1, & B. Ravitheja, Shank's Baby-Step Giant-Step Attack Extended To Discrete Log with Lucas Sequence, IOSR Journal of Mathematics (IOSR-JM, Volume 12, Issue 1, Ver.I, (Jan. - Feb. 2016), PP 09-16.
[20] W. Diffi and M. E. Helman "New directions in Cryptography." IEEE Transactions on Information theory, 22, 644654, 1976.
[21] William Stallings "Cryptography and network security principals and practice" 5th ed
[22] KomaragiriRaghavaRao et.al., An Efficeint Hybrid Model for Stegnocrypt Message Transmission, Test Engineering and Management,Vol. January – February 2020, pp. 13873 – 13879
[23] Inumula Veera Raghava Rao, et.al., Object Tracking and Object Behavior Recognition System in High Dense Crowd Videos for Video Supervision: A Review, Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018.
[24] D.Satishkumar,et.al, A Study on consumer behavior at corporate retail stores in Vijayawada city., International Conference on Applied and Computational Mathematics IOP Conf. Series: Journal of Physics: Conf. Series 1139 (2018) 012039.
[25] D. Satish kumar,et.al., Predicting Student's Campus Placement Probability using Binary Logistic Regression., International Journal of Recent Technology and Engineering (IJRTE) Vol.8(4), November 2019.