IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Review Article)

Some comparison on application of cryptology algorithms

Saeed Seyed Agha Banihashemi *

School of international relations Faculty of science and technology.

International Journal of Science and Research Archive, 2022, 05(01), 067–072

Publication history: Received on 27 December 2021; revised on 06 February 2022; accepted on 08 February

2022 Article DOI: https://doi.org/10.30574/ijsra.2022.5.1.0036

Abstract

In this article we are going to compare useful cryptology algorithm in different area and explain them though application of algorithms have very large area but doing some comparison one can do decision of usage of introduced algorithm in right place. In this article first we mention important point of, digital signature and distribution key and then we compare these tow cryptology algorithms.

Keywords: Cryptology; Algorithm; Cipher; Comparison

1. Key Distribution and key Agreement

In comparison of Public key system and private key system we know that public key is better since public key does not need safe channel and exchange of keys .But Public key system is acting slower than for that reason for long massage usually use private key system like DES in the following we explain methods which reduces these weakness .

1.1. Key Distribution of BLOM

- We make prime P and for each user U let τ_u , $\tau u \in Z_p$ are separate
- TA(trusted authority) choose three number a,b,c, belong Z_p construct

$$f(x,y)=a+b(x+y)+cxy$$

- For each user TA consider

$$g_u(x)=f(x,\tau_u)\bmod p$$

Then transfer $g_u(x)$ to U on safe channel note that $g_u(x)$ is a linear form of x so we can write
$$\begin{aligned} g_u(x) &= a_u + b_u x \\ a_u &= a + b\tau_u \bmod p \\ b_u &= b + c\tau_u \bmod p \end{aligned}$$

- If u ,v decided to contact they use common key[1]

*Corresponding author: Saeedv Seyed Agha Banihashemi
School of international relations Faculty of science and technology.

$$k_{u,v} = k_{v,u} = f(\tau_u, \tau_v) = a + b(\tau_u + \tau_v) + c\tau_u\tau_v$$

U calculate $k_{u,v}$ through $f(\tau_u, \tau_v) = g_u(\tau_v)$ and

V calculates $k_{u,v}$ through $f(\tau_u, \tau_v) = g_v(\tau_u)$.

1.2. Diffe-Hellman Distribution key

We explain only algorithm

- We P is prime and $\alpha \in Z_p^*$ will be made as public.
- V calculate $k_{u,v} = \alpha^{a_u a_v} \bmod p = b^{a_v}{}_u \bmod p$ with use of public value b_u through verification of user U with secret value of. a_v
- U calculates $k_{u,v} = \alpha^{a_u a_v} \bmod p = b^{a_u}{}_v \bmod p$ with public value of b_v from verification of user V with secret key. a_u
- Signature of TA on verification of user will not allow any change of enemy on information of user. We must worry about passive attack so question is that whether ,user we can calculate $k_{u,v}$ if. $w \neq u, v$ In other word with given value $\alpha^{a_v} \bmod p, \alpha^{a_u} \bmod p$ can calculate ? $\alpha^{a_u a_v} \bmod p$ This problem known as Diffe _Hellman Problem.

Since problem of Disconnected logarithm is difficult in Z_p so this Distribution key of Diffe-Hellman is safe. The point is here that how much this system is safe? We cannot say but we can do some comparison.

Theorem: Breaking of cryptology system of EL Gamal is equal of Diffe- Helman.[2]

1.3. Kerberos

Having a key for long time is dangerous so in this system on line will be produced by TA and time L will be considered after time L new key will be produced by TA. follow the algorithm.

- U ask a session key from TA for contact V.
- TA choose a random session key and also a time stamp T and a time line L.
- TAcalculate following values:

$$m_1 = e_{k_u}(k, ID(v), T, L)$$
$$m_2 = e_{k_v}(k, ID(u), T, L)$$

Then send m_1, m_2 to U.

- U calculate decryption function d_{k_u} for calculation of K, T, L, ID (v) from m_1 then calculate $m_3 = e_k(ID(u), T)$ and send m_2, m_3 to V.
- V use decryption function d_{k_v} to calculate K,T,L,ID(U) from m_2 then he use d_k for comparison T and ID(u) from . m_3 Then he compare two value T and ID(u) are same or not If they are same then V calculate $m_4 = e_k(T+2)$ and send it to U.

- U decryption m_4 by d_k and verify that answer is T+1.

Important point is here that Different function which will be used for massages m_1, m_2 , prepare safe area for transformation of session key K and m_3, m_4 doing verificati on that U,V have same session ky .[3]

1.4. Exchange of key (Diffe-Hellamn)

If we van not useon line production of key we use this method.

- U chooses value a_u random as such. $0 \le a_u \le p-2$
- U calculate value $\alpha^{a_u} \bmod p$ and send it to V.
- V choose value a_v random as such. $0 \le a_v \le p-2$
- V calculate value $\alpha^{a_v} \bmod p$ and send to U.
- U calculate $k=(\alpha^{a_v})^{a_u} \bmod p$ and V calculate. $k=(\alpha^{a_u})^{a_v} \bmod p$

In the end U,V can make same key. $k=\alpha^{a_u{}^{a_v}} \bmod p$

1.4.1. The station to station protocol

In this system U send massage to V in the middle W takes the massage and change it. For doing correction of this system (Diffe-Helman) we can use authenticated key agreement which called station to station protocol. [4]

- U chooserandom a_u such as. $0 \le a_u \le p-2$
- U calculates $\alpha^{a_u} \bmod p$ and sends to V.
- V chooses random a_v such as. $0 \le a_v \le p-2$
- V evaluate $\alpha^{a_u} \bmod p$ and $\begin{array}{c} k=(\alpha^{a_u})^{a_v} \bmod p \\ y_v = Sig_v(\alpha^{a_v},\alpha^{a_u}) \end{array}$ and send) C) V $\alpha^{a_v}, y_v)$,(to U.
- U evaluates. $k=(\alpha^{a_v})^{a_u} \bmod p$
- Then he verify y_v with Ver_v C (V) verify by. Ver_{TA}
- U evaluate $y_u = Sig_v(\alpha^{a_u},\alpha^{a_v})$ and send $C(U, y_u)$ to V.
- V verify y_u by Ver_v and verify C (u) by. Ver_{TA}

1.4.2. MIT key Arrangement protocols) (Mastumoto, Takadhima, Imai)

Important point of the protocol is that verification of key is not required.

- U choose τ_u randomin such a way that $0 \le \tau_u \le p-2$ and calculate. $s_u = \alpha^{\tau_u} \bmod p$
- U sends $(C(u), S_u)$ toV.
- V choose random τ_v in such a way that $0 \le \tau_v \le p-2$ and evaluate. $S_v = \alpha^{\tau_v}$
- V sends value of $C(v), S_v)$ two U.
- U calculate $k=S_v^{a_u} b_v^{\tau_v} \bmod p$ which value of b_v from C (v (andV evaluate. $k=S_u^{a_v} b_u^{\tau_u} \bmod p$ which he calculate b_u from C (u).

2. Digital signature

Another application of cryptology algorithm is to use in digital signature in this section we explain different system of cryptology which will be used in digital signature. First of all we explain a general procedure for signature then in other sections we explain different use of algorithm in signature system.[5]

A system of signature is a quandary (P, A, K.S, V) which satisfy following conditions.

- P a finite set of possible message.
- A a finite set of signature.
- K a finite set of keys.
- For $k \in K$ there exist a signature algorithm $Sig_k \in S$ which there exist a verify algorithm $Ver_k \in V$ such as

$$Sig_k : P \to A$$
$$Ver_k : P \times A \to \{true,\ false\}$$

They are functions which following equations for each signature $y \in A$

$$\begin{matrix} y = Sig(x)\ if \\ y \neq Sig(x)\ if \end{matrix}\ Ver(x,y) = \begin{cases} true \\ false \end{cases}$$

Pair (x,y) $x \in P, y \in A$,is called message signature.

Now we consider different system of signature.

2.1. System of RSA signature

Consider n=pq which p and q are prime such that . $P = A = Z_n$ We define set of space key as follow:

K$\{(n,p,q,a,b): n = pq$ =p,q are prime $ab \equiv 1 \bmod n$ $\}$, values of n,b are public key and p,q,a are private key and

$$Sig_k(x) = x^a \bmod p$$

we define $Ver_k(x,y) = true \Leftrightarrow x \equiv y^b \bmod n$

$$x, y \in Z_n$$

For protect from duplicate signature we can use Hash function.[5]

Different attack for this system are as follow:

- key-only attack
- Known massage attack
- chosen message attack
- Total break
- selective forgery
- existential forgery

2.2. System of Hash function signature

Usually in systems of signatures there is fast hash function of public cryptology. System signature with hash function is as follow:

Message x $x \in \{0,1\}^*$

Short message z=h(x) $z \in Z$

Signature $y = Sig_k(z)$ $y. \in Y$

You can see that hash function and use of short message make safe system.

2.3. El Gamal system of signature

El Gamal introduced on 1985 for first time and is improved version of DSA both signature and public key of El Gamal are non -deterministic, its algorithm are as follow

P is prime. $\alpha \in Z_p^*$, $\in Z_p$ and consider $P = Z_p^*, A = Z_p^* \times Z_{p-1}^*$ and define

α, β, P , $\alpha = \{(p, \alpha, \beta, a) : \beta \equiv \alpha^a (\bmod p)\}$ are public key ,a private key.

For $K = (P, \alpha, a, \beta)$ and for secret random number $k = Z_{p-1}^*$ we define

$$Sig_k(x,k) = (\gamma, \delta)$$
$$\gamma = \alpha^k \bmod p$$
$$\delta = (\alpha^k \bmod p) \bmod q$$

For. $x, \gamma \in Z_p^*, \delta \in Z_{p-1}$

Define. $Ver_k(x, (\gamma, \delta)) = true \Leftrightarrow \beta^\gamma \gamma^\delta \equiv \alpha^x \bmod p$ [6]

2.4. DSA system of signature

Main idea of this algorithm is from El Gamal . DSA use an ordered sub group q from , Z_q^* q is a prime number 160 bit, p a prime of L bit since . $L \equiv 0 \bmod 64, 512 \le L \le 1024$ Message before signature use HASH-1 algorithm.

Consider $\alpha \in Z_p^*$ a qth root of one module p. $A = Z_p^* \times Z_q^*, P = \{0,1\}^*$. Define

$\alpha = \{(p, q, \alpha, a, \beta) : \beta \equiv \alpha^a (\bmod p)\}$ Since $0 \le a \le q-1$.

Value P, α, β are public key and a private key for K= (p, q, α, β, a) and for A random number k, $1 \le k \le q-1$ we define

$$Sig_k(x,k) = (\gamma, \delta)$$
$$\gamma = (\alpha^k \bmod p) \bmod q$$
$$\delta = (SHA-1(x) + a\lambda)k^{-1} \bmod q$$

If $\lambda = 0 or \delta = 0$ we must choose a new random from k .For $x \in \{0,1\}^*$, $\gamma, \delta \in Z_p^*$ verification will be done by:

$$e_1 = SHA-1(x)\delta^{-1} \bmod p$$
$$e_2 = \gamma\delta^{-1} \bmod q$$
$$Ver(x, (\lambda, \delta)) = true \Leftrightarrow (\alpha^{e_1}\beta^{e_2} \bmod p) \bmod q$$

In October 2001 NIST offered P be a prime number of 1024 bit. Consider that if $\delta \equiv 0 \bmod q$ algorithm reject signature of sender and do new signature with random number k. Note that the case $\delta \equiv 0 \bmod q$ is with probability of 2^{-160} which is impossible.

3. Conclusion

In this article we claim which algorithm in cryptography is suitable for which propose so by reading this article user can find which algorithm is suitable for which propose .

References

[1] JA BUCHMANN. Introduction to cryptography .Spring-verlage. 2001.

[2] AJ MENZES, PC VAN, OORSHOT, SAVANSTONE. Hand book of Applied Cryptography.CRC. 1996.

[3] RA MOLLIN. An Introduction to cryptography .Chapman & Hall/CRC. 2001.

[4] B.SCHNEIER .Applied Cryptography, protocols, Algorithms and source code in C, second Edition. Jhon wiley and sons. 1995.

[5] DR STINSON. Cryptography, Theory and practice. Chapman &Hall/CRC. 2002.

[6] W Stallings. Cryptography and Network Security: Principles and Practice second Edition.