نخستین کنگره بین المللی
چالش های الکترونیکی ۲۰۱۶-تهران
1st Tehran eChallenges
International Congress 2016
17-18 October 2016 / ۲۶و۲۷ مهرماه ۱۳۹۵

Some comparison on application of cryptology algorithms

saeed seyed agha banihashemi
school of international realtions
ihusaied۲۰۰۱@yahoo.com

Abstract

In this article we are going to compare useful cryptology algorithm in different area and explain them though application of alogrithms have very large area but doing some comparison reader 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 tow cryptolgy algorithm ,PGP and Fortpza .

Keywords: cryptography,alghorithms,keys

۱-Key Distribution and key Agreement

In comparisoin of Public key system and private key system we know that public key is better since public key does not need safe chanel and exchenge of keys.But Public key system is acting slower than for that reason for long massage ususally use private key system like DES in the folwing we explaing methods which reduces these weekness .

۱-۲- Key Distribution of BLOM

۱)We make prime P and for each user U let $\tau u \in Z_p, \tau_u$ are separate

۲)TA(trusted autharity) choose three number a,b,c, belong Z_p construct

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

۳) For each usre TA consider

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

then trasfer $g_u(x)$ toU on safe chanel note that $g_u(x)$ is alinear form of x so we can write

$$g_u(x) = a_u + b_u x$$

$$a_u = a + b\tau_u \bmod p$$

$$b_u = b + c\tau_u \bmod p$$

٤)If u,v decied to contact they use common key

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

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

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

۱-۳ -Diffe-Hellman Distribution key

We explain only algorithm

۱) We P is prime and $\alpha \in Z_p^*$ will be made as public.

۲) 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 trough varification of user U with secret valeu of a_v .

۳) U calculate $k_{u,v} = \alpha^{a_u a_v} \bmod p = b^{a_u}{}_v \bmod p$ with public value of b_v from varification of user V with secret key a_u .

Signnature of TA on varification of user will not allow any change of enemy on information of user.We must worry about passive attack so question is that wether user w 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 caculate $\alpha^{a_u a_v} \bmod p$? 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 can not say but we can do some comparision .

Theorem: Breaking of cryptology system of ELGamal is equal of Diffe-Helman .

۱-٤-Kerberos

Having a key for long time is dangerous so in this system on line willwb produced by TA and time L will be concidered aftre time L new key will be produced by TA.Follow the algorithm

۱)U ask a session key fromTA for contact V .

۲)TA choose a random session key and also atime stamp T and atime line L.

۳)TA calculate 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.

٤) 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 .

۵)V use decryption function d_{k_v} to calculate K,T,L,ID(U) from m_2 then he use d_k for comparission 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.

٦) U decryption m_4 by d_k and varify that answer is T+١.

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 varyfication that U,V have same session key.

١-٤- Excange of key (Diffe-Hellamn)

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

١) U choose value a_u random as such $0 \le a_u \le p-2$.

٢) U calculate value $\alpha^{a_u} \bmod p$ and send it to V .

٣) V choose value a_v random as such $0 \le a_v \le p-2$.

٤) V calculate value $\alpha^{a_v} \bmod p$ and send to U.

٥) 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 same key $k = \alpha^{a_u a_v} \bmod p$.

١-٥-١The sattion to station protecol

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 protcol .

١)U choose ramdom a_u such as $0 \le a_u \le p-2$.

٢) U calculate $\alpha^{a_u} \bmod p$ and send to V.

٣)V choose random a_v such as $0 \le a_v \le p-2$.

٤) V evaluate $\alpha^{a_u} \bmod p$ and $\begin{matrix} k = (\alpha^{a_u})^{a_v} \bmod p \\ y_v = Sig_v(\alpha^{a_v}, \alpha^{a_u}) \end{matrix}$ and send $(C(V), \alpha^{a_v}, y_v)$ to U.

٥) U evaluate $k = (\alpha^{a_v})^{a_u} \bmod p$.

Then he varify y_v with Ver_v C(V) varify by Ver_{TA}.

٦)U evaluate $y_u = Sig_v(\alpha^{a_u}, \alpha^{a_v})$ and send $C(U, y_u)$ to V.

٧)V varify y_u by Ver_v and varify C(u) by Ver_{TA}.

١-٥-٢ - MIT key Arrangment protocls)(Mastumoto, Takadhima, Imai)

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

١)U choose τ_u random in such a way that $0 \le \tau_u \le p-2$ and calculate $s_u = \alpha^{\tau_u} \bmod p$.

٢)U send $(C(u), S_u)$ to V.

٣) V choose random τ_v in such a way that $0 \le \tau_v \le p-2$ and evaluate $S_v = \alpha^{\tau_v}$.

٤) V send value of $C(v), S_v)$ to U.

٥)U calculate $k = S_v^{a_u} b_v^{\tau_v} \bmod p$ which value of b_v from C(v) and V evaluate $k = S_u^{a_v} b_u^{\tau_v} \bmod p$ .which he caculate b_u from C(u).

٢-Digital signature

Another application of cryptolgy algorithem is to use in digital signature in this section we explain different system of cryptology which will be use in digital sinature . First of all we explain a general procedure for signature then in other sctions we explain different use of algorithem in signature system .

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

١-P a finite set of possible massage .

٢- A a finite set of sigintare .

٣-K a finite set of keys.

٤- For $k \in K$ there exist a signature algrithm $Sig_k \in S$ which there exist a varify 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 $y \in A$

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

pair (x,y) $x \in P, y \in A$ is called massage signiture.

Now we consider different system of signature .

٢-١- Sysetm of RSA signature

Consider n=pq which p and q are prime such that $P = A = Z_n$ .We difine 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

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

are private key and we difine $Ver_k(x, y) = true \Leftrightarrow x \equiv y^b \bmod n$

$$x, y \in Z_n$$

For protect from dublicate signiture we can use Hash fuction.

Different attack for this system are as follow:

١) key-only attack ٢) Known massage attack ٣) chosen message attack ٤) Total break

٥) selective forgery ٦) existential forgery

٢-٢- System of Hash function signature :

Usually in systems of signaturees there is fast hash fuction of public cryptology .System signture with hash fuction 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 fuction and use of short message make safe system system.

۲-۳ - ElGamal system of signature :

ElGamal intruduced on ۱۹۸۵ for first time and is improved version of DSA both signsture and public key of ElGamal are non -detrministic, Its algorithm are as follow

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

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

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

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

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

Difine $Ver_k(x,(\gamma,\delta)) = true \Leftrightarrow \beta^\gamma \gamma^\delta \equiv \alpha^x \bmod p$.

۲-۴-DSA system of signsture:

Main idea of this algorithm is from ElGamal . DSA use a ordered sub group q from Z_q^*, q is a prime number ۱۶۰ bit ,p a prime of L bit since . $L \equiv 0 \bmod 64, 512 \le L \le 1024$ Message before signiture use HASH-۱ algorithem .

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

$$\alpha = \{(p,q,\alpha,a,\beta) : \beta \equiv \alpha^a (\mathrm{mod}\ p)\} \text{ since } 0 \le a \le q-1.$$

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 ۲۰۰۱ NIST offered P be a prime number of ۱۰۲٤ bit. Consider that if $\delta \equiv 0 \bmod q$ algorithm reject signature of sendr and do new signature with arndom number k . Note that the case $\delta \equiv 0 \bmod q$ is with probability of 2^{-160} which is impossible.

Sources:

١-J.A.BUCHMANN.Introduction to cryptography.Spring-verlage ٢٠٠١.
٢-A.J.MENZES,P.C.VAN OORSHOT and S.A.VANSTONE.Hand book of Applied Cryptography.CRC ١٩٩٦.
٣-R.A.MOLLIN.An Introduction to cryptography.Chapman & Hall/CRC,٢٠٠١.
٤-B.SCHNEIER.Applied Cryptography,protocols,Algorithms and source code in C,second Edition.Jhon wiley and sons,١٩٩٥.
٥-D.R.STINSON.Cryptography,Theory and practice.Chapman &Hall/CRC ٢٠٠٢.
٦-W. Stallings.Cryptography and Network Security:Prenciples and Practice second Edition.