RSA VA EL-GAMAL OCHIQ KALITLI SHIFRLASH ALGORITMI ASOSIDA ELEKTRON RAQMLI IMZOLARI. RSA OCHIQ KALITLI SHIFRLASH ALGORITMI ASOSIDAGI ELEKTRON RAQAMLI IMZO

Sharopova Muxayyo Muxtor qizi
Osiyo Xalqaro Universiteti
“Umumtexnik fanlar” kafedrasi o‘qituvchisi
E-mail: muxayyosharopova4@gmail.com

ANNOTATSIYA

Ushbu maqolada elektron raqamli imzo haqida tushunchalar va undan foydalanishdan ko‘zlangan asosiy maqsadlar ko‘rsatilgan.

Xususan elektron imzoning asosiy xususiyatlari tuzilishiga ko‘ra turlari va kalitlarni generatsiya qilish bo‘yicha ham turli guruhlarga ajratilgan holda bayon etilgan.

Bundan tashqari elektron imzoning asosini tashkil qilgan fan “Kriptografiya ” fani haqida hamda bu fanning dastlabki shifrlash algoritmlari keltirilgan , ularga doir misollar ko‘rsatib o‘tilgan.

Bobni asosiy qismida RSA va El –Gamal algoritmiga asoslangan elektron raqamli xossalari taqdim etilgan va ularning xususiyatlari ko‘rsatib o‘tilgan.

Kalit so‘zlar: shifrlash,RSA ,El-Gamal ,Kriptografiya

ABSTRACT

This chapter describes the concept of electronic digital signature and the main goals of its use.

In particular, the main features of the electronic signature are described, divided into different groups according to the types and generation of keys according to the structure.

In addition, the science "Cryptography", which is the basis of the electronic signature, and the initial encryption algorithms of this science are given, examples of them are shown.

In the main part of the chapter, electronic digital properties based on RSA and El-Gamal algorithm are presented and their properties are shown.

Key words: shifrlash,RSA ,El-Gamal, Cryptography

KIRISH

Tizimning har bir i- foydalanuvchisi (e_i, d_i) - kalitlar juftligini yaratadi. Buning uchun yetarli katta bo‘lgan p va q - tub sonlari olinib (bu sonlar mahfiy tutiladi), $n = pq$ - soni va Eyler funksiyasining qiymati $\varphi(n)=(p-1)(q-1)$ hisoblanadi (bu son ham maxfiy tutiladi). So‘ngra, $(e_i, \varphi(n))=1$ shartni qanoatlantiruvchi, ya’ni $\varphi(n)$ -soni bilan o‘zaro tub bo‘lgan e_i -son bo‘yicha d_i-soni ushbu $e_i d_i = 1 \bmod \varphi(n)$ formula orqali hisoblanadi. Bu $(e_i; d_i)$ –juftlikda e_i - ochiq kalit va d_i - maxfiy kalit deb e’lon qilinadi.

Shundan so‘ng i- foydalanuvchidan j - foydalanuvchiga shifrlangan ma’lumotni imzolagan holda jo‘natishi quyidagicha amalga oshiriladi:

1. Shifrlash qoidasi: $M^{e_j} \bmod n = C$, bu yerda M - ochiq ma’lumot, C –shifrlangan ma’lumot;

2. Deshifrlash qoidasi: $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$;

3. ERI ni hisoblash: $H(M)^{d_i} \bmod n = P_i$,

bu yerda i- foydalanuvchining P_i- imzosi M - ma’lumotning $H(M)$- xesh funksiya qiymati bo‘yicha hisoblangan;

4. ERI ni tekshirish:

$(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$, agar $H(M) = H(M_1)$ bo‘lsa (bu yerda M_1 - deshifrlangan ma’lumot), u holda elektron hujjat haqiqiy, aks holda haqiqiy emas, chunki xesh funksiya xossasiga ko‘ra $M = M_1$ bo‘lsa ularning xesh qiymatlari ham teng bo‘ladi.

5. Ma’lumotni maxfiy uzatish protokoli:

$\left[M \cup H(M)^{d_i}\right]^{e_j} \bmod n = \left[M \cup P_i\right]^{e_j} \bmod n = C$;

6. Maxfiy uzatilgan ma’lumotni qabul qilish protokoli:

$C^{d_j} \bmod n = \left[M \cup P_i\right]^{e_j d_j} \bmod n = M \cup P_i$, umuman qaraganda dastlabki ma’lumot o‘zgartirilgan bo‘lishi mumkin, shuning uchun $C^{d_j} \bmod n = M_1 \cup P_i$

bo‘lib, natijada, xesh qiymat imzo bo‘yicha ushbu ifoda $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$ bilan hisoblanadi va qabul qilib olingan ma’lumotning xesh qiymati $H(M_1)$ bo‘lsa, u holda $H(M) = H(M_1)$ bo‘lganda elektron hujjat haqiqiy, aksincha bo‘lsa qalbaki hisoblanadi.

El-Gamal ochiq kalitli shifrlash algoritmi asosidagi ERI.

El-Gamal ochiq kalitli shifrlash algoritmiga asoslangan kriptotizimning har bir i- foydalanuvchisi uchun ochiq va maxfiy kalitlar generatsiyasi quyidagicha amalga oshiriladi, ochiq e’lon qlinadigan p_i- tub son (yoki foydalanuvchilar guruhi uchun umumiy bo‘lgan p - tub son) tanlanadi, ushbu $g_i < p_i$ (yoki foydalanuvchilar guruhi

uchun $g < p$) shartni qanoatlantiruvchi g_i (yoki foydalanuvchilar guruh uchun g) soni tanlanadi, ushbu $y_i = g^{x_i} \bmod p_i$ (p-umumiy bo‘lganda $y_i = g^{x_i} \bmod p$, $x_i < p$) formula bilan x_i - maxfiy kalit bo‘yicha y_i soni hisoblanadi. Shunday qilib, (p_i, g_i, y_i)-parametrlar birikmasi (umumiy p va g uchun (p, g, y_i)- parametrlar birikmasi ochiq kalitni tashkil etadi, maxfiy kalit x_i hisoblanadi.

Tizimda i-foydalanuvchidan j- foydalanuvchiga shifrlangan ma’lumotning imzolangan holda jo‘natilishi quyidagicha amalga oshiriladi:

1. **Shifrlash qoidasi**: $a_j = g_j^k \bmod p_j$, $b_j = y_j^k M \bmod p_j$ (umumiy p va g lar uchun $a = g^k \bmod p$, $b_j = y_j^k M \bmod p$), bu yerda k-tasodifiy son bo‘lib ma’lumotni imzolovchi tomonidan tanlanadi, bu son $(p_j - 1)$ soni bilan o‘zaro tub EKUB $(k, p_j - 1) = 1$ (p va g umumiy bo‘lganda EKUB(k, $p-1$) =1), M-ochiq ma’lumot, shifrlangan ma’lumot $(a_j, b_j) = C$ (p va g umumiy bo‘lganda, $(a, b_j) = C$).

2. **Deshifrlash qoidasi**: $b_j \big/ a_j^{x_j} \bmod p_j = M$ (p va g umumiy bo‘lganda $b \big/ a^{x_j} \bmod p = M$), haqiqatan ham $b_j \big/ a_j^{x_j} \bmod p_j \equiv g_j^{x_i k} M \big/ g_j^{k x_i} \bmod p_j \equiv M$ (p va g umumiy bo‘lganda $b \big/ a^{x_j} \bmod p \equiv y_j^k M \big/ a^{x_j} \bmod p \equiv g^{x_j k} M \big/ g^{k x_j} \bmod p = M \bmod p = M$, bunda $M < p$);

3. ERIni hisoblash qoidasi: $a_i = g_i^k \bmod p_i$, b_i soni esa $M = (x_i a_i + k b_i) \bmod (p_i - 1)$ yoki $H(M) = (x_i a_i + k b_i) \bmod (p_i - 1)$ tenglamadan topiladi, ya’ni $b_i = (M - a_i x_i) k^{-1} \bmod (p_i - 1)$ yoki $b_i = (H(M) - a_i x_i) k^{-1} \bmod (p_i - 1)$ (p va g umumiy bo‘lganda $a = g^k \bmod p$, b soni esa $M = (x_i a + k b) \bmod (p - 1)$ yoki $H(M) = (xa + kb) \bmod (p - 1)$ tenglamadan topiladi, ya’ni $b = (M - a x_i) k^{-1} \bmod (p - 1)$ yoki $b = (H(M) - a x_i) k^{-1} \bmod (p - 1)$, EKUB$(k, p-1) = 1$) $H(M)$-ma’lumotning xesh qiymati, x_i-maxfiy kalit, imzo sifatida a_i va b_i juftlik, ya’ni $(a_i, b_i) = P_i$, (p va g umumiy bo‘lganda (a, b)) imzo deb qabul qilinadi.

4. Imzoni tekshirish qoidasi:

Agar $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^M \bmod p_i$ yoki $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{H(M)} \bmod p_i$ bo‘lsa, u holda elektron hujjat haqiqiy, aks holda qalbaki hisoblanadi. Chunki,

$y_i = g_i^{x_i} \bmod p_i$ va $a_i = g_i^k \bmod p_i$

tengliklar o‘rinli bo‘lib, Ferma teoremasiga ko‘ra ushbu ayniyat o‘rinli:

$y_i^{a_i} a_i^{b_i} \bmod p_i = (g_i^{x_i})^{a_i} (g_i^k)^{b_i} \bmod p_i = g_i^{a_i x_i + k b_i} \bmod p_i = g_i^{d(p_i - 1) + M} \bmod p_i =$

$= g_i^{d(p_i-1)} g_i^M \bmod p_i = (g_i^{(p_i-1)})^d \bmod p_i \cdot g_i^M \bmod p_i (\bmod p_i) =$

$= 1^d \bmod p_i \cdot g_i^M \bmod p_i (\bmod p_i) = g_i^M \bmod p_i$;

5. Ma'lumotni maxfiy uzatish protokoli:

$a_j = g_j^k \bmod p_j$, $b_j = y_j^k M' \bmod p_j = y_j^k [M \cup P_i] \bmod p_j$, $(a_j, b_j) = C$

6. Maxfiy uzatilgan ma'lumotni qabul qilish protokoli:

$$b_j / a_j^{x_j} \bmod p_j = M' = M \cup P_i,$$

umuman qaraganda, dastlabki ma'lumot o'zgartirilgan bo'lishi mumkin, shuning uchun

$$b_j / a_j^{x_j} \bmod p_j = M' = M_1 \cup P_i,$$

bo'lib, $H(M_1)$ - xesh qiymat hisoblanadi. Agar $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{M_1} \bmod p_i$ yoki $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{H(M_1)} \bmod p_i$ bo'lsa, u holda elektron hujjat haqiqiy, aks holda qalbaki hisoblanadi.

Endi imzoni hisoblash va uni tekshirishga asoslangan ERI algoritmlari DSA va ГОСТ Р 34.10-94 standarlari bilan tanishiladi. Bu algoritmlarning asosini El-Gamal shifrlash algoritmi tashkil etadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI: (REFERENCES)

1. Karimov I. A. Mamlakatimizni modernizatsiya qilish va kuchli fuqarolik jamiyati barpo etish – ustuvor maqsadimizdir. (2010 yil 27 yanvarda bo'lib o'tgan O'zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasi va Senatining qo'shma majlisidagi ma'ruzasi. Manba: http:www.press-service.uz/uz/news/archive/ dokladi).

2 Акбаров Д. Й. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг кўлланишлари. "Ўзбекистон маркаси" нашриёти. Тошкент – 2009 йил, -398 б.

3 А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ, 2002.-480 с

4 W. Diffie and M.E. Hellman, «New directions in cryptography» IEEE Trans. Informat. Theory, vol. IT-22, pp. 644-654, Nov. 1976.

5. R. C. Merkle, «Secure communication over insecure channels», Comm. ACM, pp. 294-299, Apr. 1978.