Advanced Encryption Standart - AES

13.11.2017

128 bitlik şifreleme algoritması, 10 döngüden oluşur. Temel olarak 4 basamak kullanılır.

a. ByteSub - BS

b. ShiftRow - SR

c. MixColumn - MC

d. AddRoundKey - ARK

$$SBox = \begin{pmatrix} 199 & 5 & 2 & \cdots \\ 1 & \cdots \\ 85 & \cdots \\ \vdots & \cdots \end{pmatrix}_{16\times16}$$

Algoritma

1-) x mesajı ARK 0. anahtarı kullanarak; $x \rightarrow 128b$, $k \rightarrow 128$ bit

ARK:

$$x \rightarrow 128b \longrightarrow \begin{pmatrix} x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} \\ \vdots & \cdots \\ \vdots & \cdots \end{pmatrix}_{4\times4} \qquad k \rightarrow 128b \longrightarrow \begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ \vdots & \cdots \\ \vdots & \cdots \end{pmatrix}_{4\times4}$$

8b

$x_{0,0} = (11101101)_2 = x^7 + x^6 + x^5 + x^3 + x^2 + 1$

$GF(2^8) \rightarrow (x^8 + x^4 + x^3 + x + 1)$, çalışma uzayı (mod polinomu; normalde mod 26, burada mod (GF))

$$ARK \longrightarrow \begin{pmatrix} x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} \\ \vdots & \cdots \\ \vdots & \cdots \end{pmatrix} \oplus \begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ \vdots & \cdots \\ \vdots & \cdots \end{pmatrix}$$

2-) BS, SR, MC, ARK 1'den 9'a kadar döngü anahtarları kullanılarak

1. → BS → SR → MC → ARK → ...
   BS → . . . .
   . . . ARK

9 defa

3-) BS. SR. ARK 10. döngü anahtarı

BS:

1. → $\begin{pmatrix} a_{0,0} & \cdots \\ \vdots & \ddots \\ & & a_{3,3} \end{pmatrix}_{4\times4} \xrightarrow{SBox} \begin{pmatrix} BS_{0,0} & \cdots \\ \vdots & \ddots \\ & & BS_{3,3} \end{pmatrix}_{4\times4}$

$a_{0,0} = \underbrace{ABCD}_{\text{satırno}}\underbrace{EFGH}_{\text{sütunno}}$

0000 0001

0 1 → SBox (0,1) = 5 , $b_{0,0} = 5$

SR:

$$\begin{pmatrix} b_{0,0} & \cdots \\ \vdots & \ddots \\ & & b_{3,3} \end{pmatrix}_{4\times4} \xrightarrow{SR} \begin{pmatrix} c_{0,0} & \cdots \\ \vdots & \ddots \\ & & c_{3,3} \end{pmatrix}_{4\times4} = \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,1} & b_{1,2} & b_{1,3} & b_{1,0} \\ b_{2,2} & b_{2,3} & b_{2,0} & b_{2,1} \\ b_{3,3} & b_{3,0} & b_{3,1} & b_{3,2} \end{pmatrix}_{4\times4}$$

MC:

$$\begin{pmatrix} d_{0,0} & \cdots \\ \vdots & \ddots \\ & & d_{3,3} \end{pmatrix}_{4\times4} = \begin{pmatrix} 00000010 & \cdots\cdots 1 & \cdots\cdots 1 & \cdots\cdots 1 \\ \cdots\cdots 1 & \cdots\cdots 11 & \cdots\cdots 11 & \cdots\cdots 1 \\ \cdots\cdots 1 & \cdots\cdots 10 & \cdots\cdots 10 & \cdots\cdots 11 \\ \cdots\cdots 11 & \cdots\cdots 1 & \cdots\cdots 1 & \cdots\cdots 10 \end{pmatrix}_{4\times4} \cdot \begin{pmatrix} c_{0,0} & \cdots \\ \vdots & \ddots \\ & & c_{3,3} \end{pmatrix}_{4\times4}$$

Ödev: Son döngüde MC neden kullanılmıyor ve 192-256 b araştır.

<u>Döngü Anahtarlarının Oluşturulması</u>

$$\begin{array}{cccc} w_0 & w_1 & w_2 & w_3 \\ \end{array} \quad w_4\ w_5\ w_6\ w_7$$

$$\begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & \cdot & & k_{1,3} \\ k_{2,0} & & \cdot & k_{2,3} \\ k_{3,0} & \cdot & \cdot & k_{3,3} \end{pmatrix}$$

if i 4'ün katı değilse

$w(i) = w(i-4) \oplus w(i-1)$

else

$w(i) = w(i-4) \oplus T(w(i-1))$

$r(i) = (00000010)^{i-4/4}$

$$\begin{array}{ccccccc} \underline{w(i-1)} & & & & & & \\ a & & b & & e & & e \oplus r(i) \\ b & \longrightarrow & c & \xrightarrow{SBox} & f & \longrightarrow & f \\ c & & d & & g & & g \\ d & & a & & h & & h \end{array}$$

SBox Oluşturulması

$(\underbrace{s_7 s_6 s_5 s_4}_{\text{satır no}}\underbrace{s_3 s_2 s_1 s_0}_{\text{sütun no}})_2$

0000 0001 0. satır 1. sütun

1000 1001 8. satır 9. sütun

$$\begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}_{16\times 16}$$

$$(0000 \quad 0001) \xrightarrow{GF(2^8)\text{'deki tersi}} (0000 \quad 0000)$$

$$\qquad\qquad\qquad\qquad y_7 \cdots \quad \cdots y_0$$

$$\begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \cdot \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} z_0 \\ z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \end{pmatrix} \rightarrow SBox$$

$(11001011)_2 \rightarrow$ 12. satır 11. sütun

$GF(2^8)$'deki tersi $\longrightarrow (0000\ 0100)_2$

$\qquad\qquad\qquad y_7 \cdots \quad \cdots y_0$

$x^7+x^6+x^3+x+1 \longrightarrow x^2$

$$z = (0001\ 1111)_2 = 31 \longrightarrow SBox = \begin{array}{c|c|} & 11 \\ \hline 12 & 31 \end{array}$$

Tanım: $f(x) \in \mathbb{Z}_p(x)$, $f(x) = f_1(x).f_2(x)$

$\deg(f_1) > 0$, $\deg(f_2) > 0$

$\mathbb{Z}_2(x)$

$f_1(x) = x^3+1 = (x+1).(x^2+x+1) = x^3+x^2+x+x^2+x+1 = x^3+2x^2+2x+1 = x^3+1$

$f_2(x) = x^3+x+1$

$f_3(x) = x^3+x^2+1$

$f_4(x) = x^3+x^2+x+1 = (x+1).(x^2+1)$

x^3+x+1

000	→	0
001	→	1
010	→	x
011	→	$x+1$
100	→	x^2
101	→	x^2+1
110	→	x^2+x
111	→	x^2+x+1

$(x^2+1).(x^2+x+1) = x^4+x^3+x^2+1 = (x^2+x) \bmod (x^3+x+1)$

	001	010	011	100	101	110	111
001	001	010	011	100	101	110	111
010	010	100	110	011	001	111	101
011	011	110	101	111	100	001	010
100	100	011	111	110	010	101	001
101	101	001	100	010	111	011	110
110	110	111	001	101	011	010	100
111	111	101	010	001	110	100	011

Soru: 111'in tersi 1011 de nedir.
(x^2)

$$\begin{array}{r|l} x^3+x+1 & x^2+x+1 \\ \hline & x+1 \\ x^2+1 & \\ \hline -x = x & \end{array}$$

$= (x^2+x+1)(x+1)+x$

$x+1 = 1.x+1$ → aralarında asallık

Asimetrik - Simetrik farkı.

Simetrik-Asimetrik şifreleme algoritmaları arası fark

20.11.2017

Ayrık Logaritma Problemi - DLP

$p \to$ asal

$\beta \equiv \alpha^x \bmod p \quad \longrightarrow \quad x \equiv \log_\alpha \beta \bmod p$

α, β, p : public olmasına rağmen x'in çözülememesi problemine DLP denir

örnek: $p=11$, $\alpha=2$, $\beta=\alpha^x \bmod p$, $\beta=9$, $x=?$

i	0	1	2	3	4	5	6	7	8	9	10
α^i	1	2	4	8	5	10	9	7	3	6	1

$\hookrightarrow x=6$

$\mathbb{Z}_{11}$'de tüm elemanlar üretildiği için α primitif elemandır.

Diffie-Hellman Anahtar Değişim Protokolü

$p \to$ asal

$\alpha \in \mathbb{Z}_p \to$ primitive eleman

$p, \alpha \to$ public

Alice	Bob
$0 \leq a_A \leq (p-2)$	$0 \leq a_B \leq (p-2)$
$\alpha^{a_A} \bmod p = \beta_A$	$\alpha^{a_B} \bmod p = \beta_B$
$(\beta_B)^{a_A} \bmod p$	$(\beta_A)^{a_B} \bmod p$
$(\alpha^{a_B})^{a_A} \bmod p$	$(\alpha^{a_B})^{a_A} \bmod p$

$\longrightarrow$ K $\longleftarrow$

araya Oscar girerse

$\alpha^{a_A} \longrightarrow \alpha^{a_O} \longrightarrow$

$\longleftarrow \alpha^{a_O} \longleftarrow \alpha^{a_B}$

$\alpha^{a_A \cdot a_O}$ $\qquad$ $\alpha^{a_B \cdot a_O}$

K_{AO} $\qquad$ K_{BO}

$\to$ a_A ve a_B'nin çözülme yöntemi değil

DLP'yi Çözmek İçin Algoritmalar

Index Calculus Algorithms

adım 1: Katsayı tabanının seçilmesi

Z_p^* da bir asal sayılar alt kümesi seçilir. $(Z_p^* \rightarrow 1, 2, \ldots, (p-1))$

$S = (p_1, p_2, \ldots, p_t)$

adım 2: p_i'nin ayrık logaritmalarını hesaplayabilmek için S kümesindeki elemanların logaritmaları üzerinden lineer ilişkiler ortaya çıkarılır.

adım 2.1: $0 \leq k \leq (p-1)$ olmak üzere, $\alpha^k \bmod p$ hesaplanır

adım 2.2: α^k'yı S deki elemanların çarpımı olacak şekilde yazılır.

$$\alpha^k \equiv \prod_{i=1}^{t} p_i^{c_i}, \quad c_i \geq 0$$

$$k = \sum_{i=1}^{t} c_i \log_\alpha p_i$$

adım 2.3: $(t+c)$ denklem takımları

adım 3: S kümesinin elemanlarının logaritmasının mesuru

$0 \leq i \leq t$, $\log_\alpha p_i \bmod p$ de denklem takımlarının üzerinden (adım 2.3) çözülür.

adım 4: x'in çözülmesi

adım 4.1: $0 \leq r \leq (p-1)$

$\beta . \alpha^r \bmod p$

adım 4.2: $\beta . \alpha^r = \prod_{i=1}^{t} p_i^{d_i}, \quad d_i \geq 0$

$$x = \log_\alpha \beta = \sum_{i=1}^{t} d_i . \log_\alpha p_i - r \bmod p$$

örnek: $p = 229$, $\alpha = 6$, $\beta = 13$, $x = ?$ $\log_6 13 \bmod 229 = x$

adım 1: $\{2, 3, 5, 7, 11\}$

adım 2.1: $0 \leq k \leq p-1$, $0 \leq k \leq 228$

$\{100, 18, 12, 62, 143, 206\}$

$6^{100} \bmod 229 = 180 = 2^2 . 3^2 . 5$

$6^{18} \bmod 229 = 176 = 2^4 . 11$

$6^{12} \bmod 229 = 165 = 3.5.11$

$6^{62} \bmod 229 = 154 = 2.7.11$

$6^{143} \bmod 229 = 198 = 2.3^2.11$

$6^{206} \bmod 229 = 210 = 2.3.5.7$

adım 2.2:

$100 = 2.\underbrace{\log_6 2}_{\to a} + 2\underbrace{\log_6 3}_{\to b} + \underbrace{\log_6 5}_{\to c}$

$18 = 4.\log_6 2 + \log_6 11$

$12 = \log_6 3 + \log_6 5 + \log_6 11$

$62 = \log_6 2 + \log_6 7 + \log_6 11$

$143 = \log_6 2 + 2.\log_6 3 + \underbrace{\log_6 11}_{\to e}$

$206 = \log 2 + \log 3 + \log 5 + \underbrace{\log 7}_{\to d}$

adım 2.3: 6 denklem, 5 değişken ✓

adım 3: $a = 21$, $b = 208$, $c = 98$, $d = 107$, $e = 162$

adım 4: $r = 77$

$\beta . \alpha^r = 13 . 6^{77} \bmod 229 = 147 = 3.7^2$

$x = \log_6 13 = \log_6 3 + 2 . \log_6 7 - 77$

$x = 117$

Shanks Algorithm

p, α, β , $x = \log_\alpha \beta \bmod p$, $m = \lceil (p-1)^{1/2} \rceil$

adım 1: $0 \leq j \leq (m-1)$, $\alpha^{mj} \bmod p$ hesapla

adım 2: $(j, \alpha^{mj} \bmod p) \mid L_1$

adım 3: $0 \leq i \leq (m-1)$ olmak üzere $\beta . \alpha^{i} \bmod p$ hesaplanır.

adım 4: $(i, \beta . \alpha^{-i} \bmod p) \mid L_2$

adım 5: $(j, y) \in L_1$ ve $(i, y) \in L_2$ bulunur

adım 6: $x = \log_\alpha \beta = (mj + i) \bmod (p-1)$

örnek: $p = 809$, $\alpha = 3$, $\beta = 525$, $x = ?$

$m = \lceil \sqrt{808} \rceil = 29$

adım 1: $\alpha^m = 3^{29} \bmod 809 = 99$

adım 2: $0 \leq j \leq 28$, $(j, 99^j \bmod 809)$

$(0,1), (1,99), (2,93), (3,308), (10,644), (11,654), (28,81), \ldots \mid L_1$

adım 3: $0 \leq i \leq 28$, $(i, 525 . 3^{-i} \bmod 809)$

adım 4: $(0,525), (1,175), (2,328), (19,644), \ldots$

adım 5: $(10,644)$, $(19,644)$

adım 6: $x = \log_3 525 = (29.10 + 19) = 309$

Pohling - Hellman Algorithm

$p \to$ prime , $p-1 = \prod_{i=1}^{n} q_i^{c_i}$

$\forall q_i \ (1 \leq i \leq n)$.

$\log_\alpha \beta \mod q_i^{c_i} = \sum_{k=0}^{c_i-1} a_i . q_i^k$ olmak üzere $a_0, a_1, ..., a_{c_i-1}$ hesaplanır.

adım 1: $0 \leq j \leq q_i-1$ için $r_j = \alpha^{(p-1).j/q_i} \mod p$

adım 2: $k=0$, $\beta_k = \beta$

adım 3: while $k \leq c_i-1$ do

a. $\delta = \beta^{(p-1)/q_i^{k+1}} \mod p$

b. $\delta = \gamma_j$ olacak şekilde j bulunur.

c. $a_k = j$

d. $\beta_{k+1} = \beta_k . \alpha^{-a_k . q_i^k} \mod p$

e. $k = k+1$

$\log_\alpha \beta \mod q_i^{c_i}$, $(1 \leq i \leq n)$

Çinli kalanlar teoremi uygulanır.

$\prod_{i=1} q_i^{c_i}$ modülünde $\log_\alpha \beta$ 'yı verir.

örnek: $p = 29$, $\alpha = 2$, $\beta = 18$, $x = ?$

$29-1 = 28 = 2^2 . 7$ $\quad q_i = 2, 7 \quad c_i = 2, 1$

El-Gamal Public Key Cryptosystem

27.11.2017

$p \to$ prime

$\alpha \in Z_p^* \to$ primitif eleman

$P = Z_p^*$, $\quad C = Z_p^* \times Z_p^*$

$K = \{(p, \alpha, a, \beta) : \beta = \alpha^a \pmod p\}$

p, α, β : public

a : private key

$\to$ Bob

$k \in Z_{p-1}$ olmak üzere bir değer seçer

$x \in P$

$e_k(x, k) = (y_1, y_2)$

$y_1 = \alpha^k \mod p$

$y_2 = x\,\beta^k \mod p$

$(y_1, y_2) \in C$

$\to$ Alice

$$x = d_k(y_1, y_2) = y_2 . (y_1^a)^{-1} \mod p$$

Araya giren kişi x'i çözebilmesi için a'yı bilmeli.

örnek $p = 2579$, $\alpha = 2$, $a = 765$

Bob:

$\beta = \alpha^a \mod p = 2^{765} \mod 2579 = 949$

2579, 2, 949 : public

765 : private

Alice

$x = 1299$

$k = 853$

$e_k(x, k) = (y_1, y_2)$

$y_1 = \alpha^k \mod p = 2^{853} \mod 2579 = 435$

$y_2 = x . \beta^k \mod p = 1299 . 949^{853} \mod 2579 = 2396$

$(y_1, y_2) = (435, 2396)$

Bob:

$x = d_k(y_1, y_2) = y_2 . (y_1^a)^{-1} \mod p$

$x = 2396 . (435^{765})^{-1} \mod 2579$

$x = 1299$

Soru: Araya giren kişi x_1 biliyorsa, x_2 bilebilirmi?

Alice → x_1, x_2 ve p, α, β, k

$e_k(x_1, k) = (y_1, y_{11})$

$e_k(x_2, k) = (y_2, y_{22})$

$y_1 = \alpha^k \bmod p$ $\quad y_{11} = x_1 . \beta^k \bmod p$

$y_{22} = x_2 . \beta^k \bmod p$

$\beta^k = \frac{y_{11}}{x_1}$ $\quad \beta^k = \frac{y_{22}}{x_2}$

$\frac{y_{11}}{x_1} = \frac{y_{22}}{x_2}$ $\quad x_2 = \frac{x_1 . y_{22}}{y_{11}}$ → x_2 bilinebilir. (y_{22} ortam dinleyerek biliniyor.)

RSA Cryptosystem

Asal çarpanlarına ayırma probleminin zorluğuna dayanır.

$n = p.q$

$P = C = \mathbb{Z}_n$

$k = \{(n, p, q, a, b) : a.b \equiv 1 \bmod \varphi(n)\}$ → Bob

n, b : public

p, q, a : private

$y = e_k(x) = x^b \bmod n$ | Alice

$x = d_k(y) = y^a \bmod n$ | Bob

Soru: $y^a \bmod n$, x'e nasıl eşit olur?

$= (x^b)^a \bmod n$

$= x^{a.b} \bmod n$

$= x^{t.\varphi(n)+1} \bmod n$

$= (\underbrace{x^{\varphi(n)}}_{1})^t . x \bmod n = 1^t . x \bmod n = x \bmod n$

örnek: $p=101$, $q=113$

Bob:

$n = p\,q = 101 \cdot 113 = 11413$

$\gcd(b, \phi(n)) = 1$ olmalı

$\phi(n) = (p-1)\cdot(q-1) = 100 \cdot 112 = 11200 = 2^6 \cdot 5^2 \cdot 7$ b; 2,5,7'ye bölünmemeli

$b = 3533$

$b^{-1} \bmod \phi(n) \rightarrow 3533^{-1} \bmod 11200 = 6597 = a$

$(11413, 3533)$: public

Alice:

$x = 9726$

$y = e_k(x) = x^b \bmod n = 9726^{3533} \bmod 11413 = 5761$

Bob:

$x = d_k(y) = y^a \bmod n = 5761^{6597} \bmod 11413 = 9726$

Ödev 11: AES 256 bit, Diffie-Hellman 512 bit, RSA 512 bit, El Gamal 512 bit, DLP'yi çözmeye yönelik algoritmalardan biri.

Soru: Alice x'i encrypt edip boblara gönderir Bob1, Bob2 ... aynı mesajı gönderdi, public'ler farklı. Bu mesajı, araya giren kişi çözebilir mi?

$x = y_1$

$x = y_2$ $y_1, y_2, \ldots$ 'ler aralarında asal ise CRT ile çözülebilir.

$\vdots$

Tanım: $p \to$ tek asal sayı olmak üzere

$a \to \mathbb{Z}_p$'de Quadratic Residue

eğer $a \not\equiv 0 \mod p$ ve $y^2 \equiv a \mod p$ $(y \in \mathbb{Z}_p)$

örnek: $\mathbb{Z}_{11}$'de QR, QNR?

$$\begin{array}{rcl} & & \underline{a} \\ 1^2 &=& 1 \\ 2^2 &=& 4 \\ 3^2 &=& 9 \\ 4^2 &=& 5 \\ 5^2 &=& 3 \\ 6^2 &=& 3 \\ 7^2 &=& 5 \\ 8^2 &=& 9 \\ 9^2 &=& 4 \\ 10^2 &=& 1 \end{array}$$

QR: $\{1, 3, 4, 5, 9\}$

QNR: $\{2, 6, 7, 8, 10\}$

Euler Kriter: Seçilen bir sayının ilgili uzayda QR olup olmadığını test etme

$p \to$ tek asal sayı

$a \to \mathbb{Z}_p$'de QR $\iff a^{(p-1)/2} \equiv 1 \mod p$

Fermat: $a = y^2$

$$(y^2)^{(p-1)/2} = y^{p-1} \mod p = 1$$

Tanım: $p \to$ tek asal sayı

$(a/p) \to$ legendre symbol

$$(a/p) = \begin{cases} 0 & \text{if } a \equiv 0 \mod p \\ 1 & \text{if } a \to \mathbb{Z}_p\text{'de QR} \\ -1 & \text{if } a \to \mathbb{Z}_p\text{'de QNR} \end{cases}$$

Tanım: $n \to$ tek pozitif tam sayı olsun

$n = \prod_{i=1}^{k} p_i^{e_i}$, p'ler asal çarpan

$(a/n) \to$ Jacobi Symbol

$$a/n = \prod_{i=1}^{k} (a/p_i)^{e_i}$$

örnek: $\frac{6278}{9975} = ?$

$9975 = 3 . 5^2 . 7 . 19$

$$\frac{6278}{9975} = \frac{6278}{3}^{\text{mod } 3=2} . \left(\frac{6278}{5}\right)^{2\ \text{mod } 5=3} . \frac{6278}{7}^{\text{mod } 7=6} . \frac{6278}{19}^{\text{mod } 19=8}$$

$$= \frac{2}{3} . \left(\frac{3}{5}\right)^2 . \frac{6}{7} . \frac{8}{19}$$

$$= -1 . (-1)^2 . -1 . -1 = -1$$: Jacobi Symbol

Solovay Strassen: Seçilen bir sayının asal olup olmadığını test eder.

$1 \leq a \leq (n-1)$

$x \leftarrow (a/n)$

if $x=0$
 then return ("n is composite")

$y \leftarrow a^{(n-1)/2} \bmod n$
if $x \equiv y \bmod n$
 then return ("n is prime")
 else return ("n is composite")

04.12.2017

Jacobi Symbol - (a/n) : $a/n = ?$

1-) if $n \rightarrow$ pozitif tek tamsayı ve $m_1 \equiv m_2 \bmod m$, then

$m_1/m \equiv m_2/m$

2-) if $n \rightarrow$ pozitif tek tamsayı, then

$$2/n = \begin{cases} 1 & , \text{ if } n \equiv \mp 1 \bmod 8 \\ -1 & , \text{ if } n \equiv \mp 3 \bmod 8 \end{cases}$$

3-) if $n \rightarrow$ pozitif tek tamsayı, then

$m_1.m_2/m = (m_1/m).(m_2/m)$

if $m = 2^k . t$ ve $t \rightarrow$ tek sayı

$m/n = (2/n)^k . (t/n)$

4-) m ve n pozitif tek tamsayı, then

$$m/n = \begin{cases} -(n/m) & , \text{ if } n \equiv m \equiv 3 \bmod 4 \\ n/m & , \text{ else} \end{cases}$$

örnek: $\dfrac{7411}{9283} = ?$

4. $= -\dfrac{(9283)}{7411}$	1. $= -\dfrac{(1872)}{7411}$	3. $= -\left(\dfrac{2}{7411}\right)^4 \dfrac{117}{7411}$
2. $= -\left(\dfrac{117}{7411}\right)$	4 $= -\dfrac{7411}{117}$	1. $= \dfrac{-40}{117}$
3. $= -\left(\dfrac{2}{117}\right)^3 \dfrac{5}{117}$	2. $= \dfrac{5}{117}$	4. $= \dfrac{117}{5}$
1 $= \dfrac{2}{5}$	2. $= -1$	

Miller - Robin (n): Asallık.

$n-1 = 2^k . m$, $m \to$ tek

rastgele a tam sayısı, $1 < a \leq (n-1)$

```
b ← a^m mod n

if  b ≡ 1 mod n  then
    return ("n is prime")

for  i ← 0  to  k-1
    if  b ≡ -1 mod n  then
        return ("n is prime")
    else
        b ← b^2 mod n

return ("n is prime")
```

örnek: $n = 29$?

$29 - 1 = 2^2 . 7$

$a = 10$ için 29 asaldır.

Özetleme Fonksiyonları

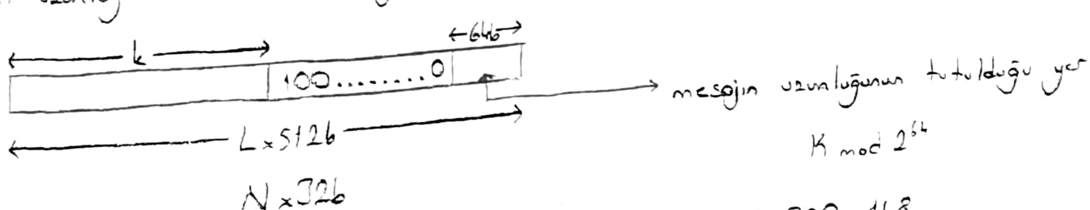
Hash fonksiyonları şifreleme algoritması değildir. Tek yönlüdürler. Şifrelemede encrypt ve decrypt olduğu için hash'ler şifreleme algoritması değildir.

Örneğin; MD5 → çıktısı 128 bittir.

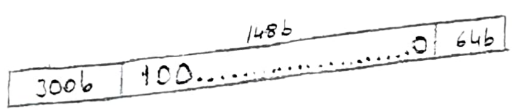
Hash Fonksiyonları

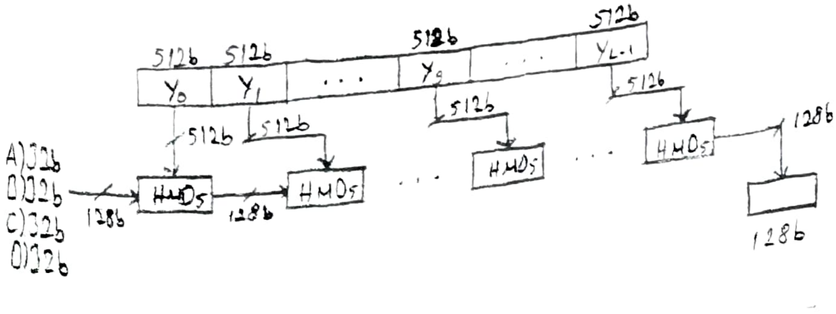
- Uzunlukları farklı olan verileri sabit uzunlukta bir çıktıya dönüştürmelidir.
- Özet değerinden mesajı elde etmek zor olmalıdır.
- MD, message digits
  - MD5 : 512 bitlik bloklara ayrılır. çıktısı 128b.
- SHA, secure hash algorithm
  - SHA-1 : 512 bitlik bloklara ayrılır, çıktısı 160b.
  - SHA-2
  - SHA-3

Eğer bit uzunluğu 512'nin katı değilse "padding" işlemi uygulanır.

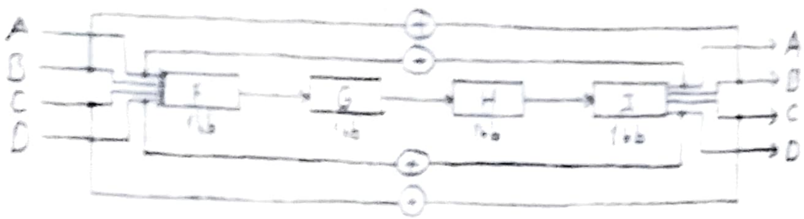


örnek: 300 bit veri, 300'ün son 64 biti, $512-64=448-300=148$





MD5 de toplam 4 adım vardır. Her adım içinde 16 adım vardır 4×16=64 adımdan oluşur.
Her bir döngüye input olarak A-B-C-D girmektedir.



128+32=160
(E)

Ödev MD5 ve SHA-1 nedir, incele.

En güvenli hash fonksiyonu

<u>Digital İmza Algoritmaları</u>

authenticate - kredi kartı imzası

(P, A, K, S, V)

P mesajların sonlu kümesi

A imzaların sonlu kümesi

K anahtar uzayı

S imzalama kuralı $\quad sig_K \in S$

V verification kuralı $\quad ver_K \in V$

$sig_K : P \to A$

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

$$x \in P \qquad ver(x, y) = \begin{cases} true, & \text{if } y = sig(x) \\ false, & \text{if } y \neq sig(x) \end{cases}$$
$$y \in A$$

Kredi kartı şifresi girilince gerçekleşen olaylar:

1-) Bir mesajı imzalama

- M mesajı hash'li fonksiyondan geçirilerek H özet değeri elde edilir.
- Elde edilen H özet değeri, gönderenin gizli anahtarıyla şifrelenerek S imzası elde edilir.
- Elde edilen S, mesaja eklenerek, imza üretilir.

$\{M, S\}$

2-) İmzalanmış mesajın doğrulanması

- $\{M, S\}$ ayrılır.
- M, hash fonksiyondan geçirilir. → H' elde edilir.
- Gönderenin açık anahtarıyla $S \rightarrow H''$
- Eğer $H' = H''$ ise true
  else false

RSA İmza Algoritması

11.12.2017

$n = p.q$, p, q : asal

n, b : public
p, q, a : private

$P = A = \mathbb{Z}_n$

$K = \{(n, p, q, a, b) : n = p.q, \ a.b \equiv 1 \mod \phi(n)\}$

$\phi(n) = \phi(p.q) = \phi(p).\phi(q) = (p-1).(q-1)$

$y = sig_K(x) = x^a \mod n$

$(x, y) \rightarrow$

$ver_K(x, y) = true \iff x = y^b \mod n$

El-Gamal Dijital İmza Algoritması

$x \to$ prime

$\alpha \in \mathbb{Z}_p^*$, $A = \mathbb{Z}_p^* \times \mathbb{Z}_{p-1}$

p, α, β : public
a : private

$K = \{(p, \alpha, a, \beta) : \beta = \alpha^a \bmod p\}$

rasgele k seçilir, $k \in \mathbb{Z}_{p-1}^*$

$sig_K(x,k) = (\gamma, \delta)$

$\gamma = \alpha^k \bmod p$

$\delta = (x - a.\gamma).k^{-1} \bmod (p-1)$

$(x, (\gamma, \delta)) \to$

$ver_K(x, (\gamma,\delta)) = true \iff \beta^\gamma . \gamma^\delta = \alpha^x \bmod p$

örnek: m = "one" (01 = a , 02 = b , ...) $p = 225119$, $\alpha = 11$, $a = 141421$, $\beta = \alpha^a \bmod p = 18191$

$x =$ "151405"

$k = 239$

$p, \alpha, \beta \to (225119, 11, 18191)$

$sig_K(x,k) = (\gamma, \delta)$

$\gamma = \alpha^k \bmod p = 11^{239}\ 225119 = 164130$

$\delta = (x - a.\gamma).k^{-1} \bmod (p-1) = (151405 - 141421.164130).239^{-1} \bmod 225118 = 187104$

$ver_K(x, (\gamma,\delta)) = true \iff \beta^\gamma . \gamma^\delta = \alpha^x \bmod p$

$(18191)^{164130}.(164130)^{187104} = (11)^{151405} \bmod 225119$ ✓

ispot: $\beta^\gamma . \gamma^\delta = \alpha^x$

$\delta = (x - a.\gamma).k^{-1}$

$x = a.\gamma + k.\delta \quad \longrightarrow \quad \alpha^{a.\gamma} . \alpha^{k.\delta} = \alpha^x = \alpha^{a.\gamma + k.\delta}$

not: k'nın p-1'de tersi olabilmesi için, k ile p-1 aralarında asal olmalı.

örnek: $p=467$, $\alpha=2$, $a=127$, $\beta=132$, $x=100$, $k=233$, İmzası ?

$p-1=466$

k ile $p-1$, 233 ile 466 aralarında asal değildir.

Schnorr İmza Algoritması

$p \rightarrow$ prime, $q \rightarrow$ prime

$\alpha \in \mathbb{Z}_p^*$

$A = \mathbb{Z}_q \times \mathbb{Z}_q$

$K = \{(p,q,\alpha,a,\beta) : \beta = \alpha^a \bmod p\}$

$0 \leq a \leq (q-1)$

p,q,α,β : public
a : private

$h : \{0,1\}^* \rightarrow \mathbb{Z}_q$

$K = (p,q,\alpha,a,\beta)$

$1 \leq k \leq (q-1)$

$sig_K(x,k) = (\gamma,\delta)$

$\gamma = h(x \,||\, \alpha^k)$

$\delta = k + a \cdot \gamma \bmod q$

$(x,(\gamma,\delta)) \rightarrow$

$ver_K(x,(\gamma,\delta)) = true \iff h(x \,||\, \alpha^{\delta} \cdot \beta^{-\gamma}) = \gamma$

Dijital İmza Algoritması - DSA

$p \rightarrow l$ bitlik asal

$l \equiv 0 \mod 64$ ve $512 \leq l \leq 1024$

$q \rightarrow 160$ bitlik prime

$x \in \mathbb{Z}_p^*$

$P = \{0,1\}^*$

$A = \mathbb{Z}_q^* \times \mathbb{Z}_q^*$

$K = \{(p, q, \alpha, a, \beta) : \beta = \alpha^a \mod p\}$

$0 \leq a \leq (q-1)$

p, q, α, β : public
a : private

$1 \leq k \leq (q-1)$

$sig_K(x, k) = (\gamma, \delta)$

$ver_K(x, (\gamma, \delta)) = true \Leftrightarrow (\alpha^{e_1} . \beta^{e_2} \mod p) \mod q = \gamma$

$e_1 = SHA\text{-}1(x) . \delta^{-1} \mod q$

$e_2 = \gamma . \delta^{-1} \mod q$

$\gamma = (\alpha^k \mod p) \mod q$

$\delta = (SHA\text{-}1(x) + a . \alpha) . k^{-1} \mod q$

örnek: $p = 7879$, $q = 101$, $\alpha = 170$, $a = 75$, $\beta = \alpha^a \mod p = 4567$, $k = 50$, $SHA\text{-}1(x) = 22$

$\gamma = (170^{50} \mod 7879) \mod 101 = 94$

$\delta = (22 + 75.94) . 50^{-1} \mod 101 = 97$

$(x, (94, 97)) \rightarrow$

$e_1 = 22 . 97^{-1} \mod 101 = 45$

$e_2 = 94 . 25 \mod 101 = 27$

$(170^{45} . 4567^{27} \mod 7879) \mod 101 = 94 \stackrel{\checkmark}{=} \gamma = 94$

Ödev: DSA, Elliptic Curve - El Gamal, Diffie-Helman, DSA; kodlar ed'ye, ciktilar finale.

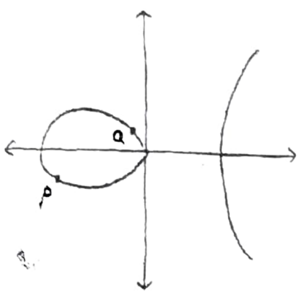
Elliptic Curve - DSA

$a, b \in R$

$4a^3 + 27b^2 \neq 0$

$(x, y) \in \mathbb{R} \times \mathbb{R}$

$E = (y^2 = x^3 + ax + b)$



P ve Q noktasının toplamı eğri üzerinde bir nokta,

P ve P " " " " " ",

Q ve Q " " " " " "

Special point, O : sonsuzdaki bir nokta

$P + O = O + P = P$

$P + (-P) = O$

$P(x_1, y_1)$, $Q(x_2, y_2)$

Case'ler:

1. $x_1 \neq x_2$
2. $x_1 = x_2$ ve $y_1 = -y_2$
3. $x_1 = x_2$ ve $y_1 = y_2$

1. $x_1 \neq x_2$

$P + Q = R(x_3, y_3)$

$y = \lambda . x + V$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ $\qquad V = y_1 - \lambda . x_1 = y_2 - \lambda . x_2$

$E \cap L$, L = eğim

$(\lambda x + V)^2 = x^3 + ax + b$, $\qquad x^3 - (\lambda x)^2 + (a - 2\lambda V)x + b - V^2 = 0$

$x_3 = \lambda^2 - x_1 - x_2$, $\qquad y_3 = \lambda(x_1 - x_3) - y_1$, $\qquad \lambda = \frac{-y_3 - y_1}{x_3 - x_1}$

2. $x_1 = x_2$ ve $y_1 = -y_2$

$P + (-P) = (x, y) + (x, -y) = O$

3. $x_1 = x_2$ ve $y_1 = y_2$

$2y \frac{dy}{dx} = 3x^2 + a$, $\qquad \lambda = \frac{dy}{dx} = \frac{3x^2 + a}{2y}$