Subject:

Subject: ۹۵۳۰۴۸۳ مهدی محمدی حامی

Year. Month. Date. ( )

۱- با استفاده از استقرای قوی:

فرض قوی:

$1 = 2^0$

$\forall\ i < k : \quad i = \sum_{j=0}^{m} 2^j$

بنابراین عدد k را می‌توان به صورت زیر نمایش داد:

$k = \underbrace{k-1} + 1 = k-1+2^0$

طبق فرض استقرا این قسمت را می‌توان نمایش داد

و همچنین داریم: $2^j + 2^j = 2\times 2^j = 2^{j+1}$

۲- می‌توان 2^a+1 را به شکل زیر نوشت:

فرض کنیم 2^a+1 بخش‌پذیر باشد بر 2^b-1 که:
همچنین از بین تمام a های ممکن کوچک‌ترین را انتخاب می‌کنیم

$2^a+1 = (2^b-1)m + r$

که r نیز بر 2^b-1 بخش‌پذیر است و برابر صفر است.

$2^a+1 = (2^b-1)(2^{a-b}) + \underbrace{2^{a-b}+1}$

حال r خود نیز به شکل $2^{\alpha}+1$ است که $\alpha < a$ است و با شرط کوچک‌ترین a

تناقض دارد پس فرض خلف باطل است و نمی‌توان 2^a+1 را بر 2^b-1 تقسیم کرد

۳ـ باقی‌مانده‌ی این عدد اول بر 3 برابر 1 است. (لزوماً $3k+1$ است)

پس باقی‌مانده‌ی این عدد بر 6 می‌تواند 1 باشد یا 4

حال آنکه اعداد زوج $6k+4$ برابر بر 2

بخش‌پذیرند پس اول نیستند. پس عدد ما می‌تواند فقط $6k+1$ باشد.

۴ـ دو عدد برابر 1 یا $p-1$ باشند

$$(p-1)^2 \bmod p = 1$$
$$1^2 \bmod p = 1 \Rightarrow (p-1)^{-1} = (p-1), \quad 1^{-1} = 1$$

ولی هیچ عدد دیگری در مجموعه‌ی Z_p^* وارون اش خودش نیست.

از آنجایی که هر عضو Z_p^* فقط یک وارون دارد، پس در مجموعه‌ی $[2, \ldots, p-2]$

اعضا به شکل دو به دو وارون یکدیگر هستند

پس $\prod_{i=2}^{p-2} i$ در پیمانه‌ی p هم برابر 1 است.

پس $(p-1)! = (p-2)!\,(p-1)$ که مقدار $(p-2)!$ در پیمانه‌ی p هم

1 است. پس $(p-1)! \bmod p = p-1$

$$\Rightarrow (p-1)! + 1 \bmod p = 0$$

Subject:

Subject:

Year. Month. Date. ( )

مهدی علی‌حاجی ۹۵۳۰۴۸۳

د-

a) $\varphi(p^a) = p^a \times (1-\frac{1}{p}) = p^a - p^{a-1}$

$= p^{a-1}(p-1)$

b) $\varphi(mn) = mn \times \prod (1-\frac{1}{p_i})$ → عوامل اول mn

$= mn \times \prod (1-\frac{1}{M_i}) \times \prod (1-\frac{1}{N_i}) \times \frac{1}{\prod (1-\frac{1}{S_i})}$

M_i ← عوامل اول m

N_i ← عوامل اول n

S_i ← عوامل اول هم n و هم m

$= \varphi(m) \times \varphi(n) \times \frac{1}{\prod (1-\frac{1}{S_i})}$

S_i ← عوامل مشترک n , m

$= \varphi(m) \times \varphi(n) \times \frac{d}{d \times \prod (1-\frac{1}{S_i})} = \varphi(m) \times \varphi(n) \times \frac{d}{\varphi(d)}$

c) $a | b \Rightarrow b = ma \Rightarrow \varphi(b) = \varphi(a)\varphi(m) \times \frac{d}{\varphi(d)}$

$d = \gcd(m, a)$

$= \varphi(a) \times m \times \prod (1-\frac{1}{M_i}) \times \frac{d}{d \times \prod (1-\frac{1}{D_i})}$

M_i: عوامل اول m — D_i: عوامل اول d

تمامی عوامل d، داخل m نیز هستند پس $\prod (1-\frac{1}{D_i})$ با $\prod (1-\frac{1}{M_i})$ ساده می‌شود

$$\varphi(b) = \varphi(a) \times m \times \prod \left(1 - \frac{1}{X_i}\right)$$

عوامل اول m منهای عوامل اول α

تمامی مقادیر X داخل m وجود دارد زیرا X ها عوامل m هستند. پس می‌توان

$m \times \prod \left(1 - \frac{1}{X_i}\right)$ را یک α در نظر گرفت که یک عدد صحیح است.

$$\varphi(b) = \varphi(a)\,\alpha \Rightarrow \varphi(a) \mid \varphi(b)$$

6

gcd(9530483, 9520231) =

gcd(9520231, 10252) =

gcd(10252, 6375) = gcd(6375, 3877) =

gcd(3877, 2498) = gcd(2498, 1379) =

gcd(1379, 1119) = gcd(1119, 260) =

gcd(260, 79) = gcd(79, 23) = gcd(23, 10)

gcd(10, 3) = gcd(3, 1) = gcd(1, 0) = 1

Subject:

Subject:

Year. Month. Date. ( )

مهدی علی حامی

7

RSA توسط $\frac{1\times10^6 \times 8 \text{ kbit}}{100 \text{ kbit/sec}} = 8\times10^4 \text{ sec}$

AES توسط $\frac{1\times10^6 \times 8 \text{ kbit}}{17\times10^3 \text{ kbit/sec}} = 470.5 \text{ sec}$

استفاده از کلید Asymmetric مزیت های خود را دارد. مثلاً در یک شبکه با n سیستم در سیستم های کلید متقارن نیاز به $\frac{n\times(n-1)}{2}$ کلید است ولی در سیستم های کلید نامتقارن تنها نیاز به $2n$ کلید است که مدیریت و استفاده از این تعداد کم کلید راحت تر است.

همچنین لازم است کلیدهای متقارن یک بار کانال امن انتقال یابند، و انتقال کلید خود در اینجا به مسئله ی مهمی می شود. درحالی که این مسئله برای کلید نامتقارن صدق نمی کند.