

مَدْحُونٌ: يَأْتِي مَهْرَبَنَ سُورِيَا (مُدْلِعٌ عَلَى)

امہ حسن رائے

Environnement

$$\begin{array}{ccc} \omega_1^x = h & \xrightarrow{\text{def}} & \omega_1^y y = h \\ \omega_1^y = h & \xrightarrow{\text{def}} & \omega_1^y x = h \end{array}$$

سؤال اول :  
صيغة التحريك سؤال دائم له :

$$\left\{ \begin{array}{l} \text{If } (a, b) = 1 \Rightarrow \text{There exist integers } x, y \\ \text{such that } ax + by = 1 = \gcd(a, b) \end{array} \right.$$

$$h^{an+by} = w_1^{bxy} w_r^{ayx}$$

$$h = w_1 b^x y w_r a y^x$$

$$\int_{\gamma}^{\beta} w_1^{b\alpha y} w_r^{a\gamma x} = (w_1^b w_r^a)^{y\alpha} = h$$

xy-th root of h is  $w_1^b w_p^a$

where  $ax+by=1$  according to  $\gcd(a,b)=1$

حکم مخواهی از افراد و اعماق اینها

سازمانی: ①

(a) سازمانی است که همان یک میریمه از افراد ساخت و سبب احتدام  
در هر کی از این دو میریمه، و میرد با شود افراد را در این نسبت توجه شده و سری از آنها  
حسب رعایت شرکت اسلام از حمله ای را میگیرند و اینها را dangerous, passenger, securities میگویند.

(b) بعد از برداشتن این افراد از این اتفاقات نشانه از هر دوسته، صراحتی  $x^a$  hash  
سازمانی خواهد بود که جمیع افرادی که عضو این اعماق میباشند  
ناظم  $x$  را میگیرند به اینکه از این دوسته بودند شاهدند.

بله اینها ساریوی مودتیاز هستند علیه این

$X_s$ ,  $X_a$  را میگیرند از dangerous, passenger, securities از حمله ای را ترسیم میکنند.

-) حال دو زیرسازمانی از اینها هستند airline, Security

$$K_{sharing} = \{ (H(k_i))^{X_a} \bmod N \text{ for } i \text{ in range}(1, m+1) \}$$

$$S_{sharing} = \{ (H(s_i))^{X_s} \bmod N \text{ for } i \text{ in range}(1, n+1) \}$$

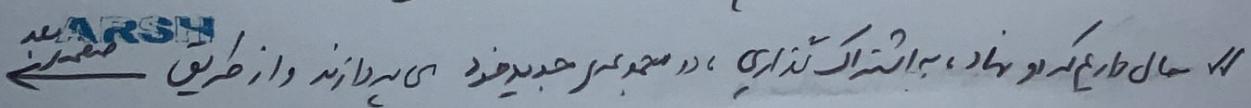
$X_a$  airline بودن و توجه امنیتی را

$X_s$  security = =

حال دو زیرسازمانی فوق همانند اینها شود و حال جستی علیه اینها:

Security gets  $K_{sharing}$   $\xrightarrow{\text{calculated}}$   $\{ (item)^{X_s} \bmod N \text{ for item in } K_{sharing} \}$

Airline gets  $S_{sharing}$   $\xrightarrow{\text{calculated}}$   $\{ (item)^{X_a} \bmod N \text{ for item in } S_{sharing} \}$

ARSH  بررسی این اثبات را در اینجا نمایم و میتوانید مجدد شدیده باشید

پس intersection ها را می بینیم که دو مجموعه را دارند، به یعنی انتها (ریاضیات) برای این دو مجموعه را می بینیم، به این انتها (ریاضیات) برای این دو مجموعه را می بینیم.

ترکیب خواهد بود، سیار سخت خواهد بود

این در استادیونه، مایل است Diffie-Hellman را در آن استفاده نماید.

صُوْلَهْتَرْاهْ كَهْرَمْ سَاتْ زِيرْ بَايدِرْ رِهْامْتْ سُونْدَهْ

- ۱- همچو سر برای از آنها بـ سانسرا باشند همانند مطلع شود

۲- اگر سخنی زدن را سُکِّر، اگر اصرار دله از آنها و مهارت استفاده کنند.

۳- آنچه نیز موقت تصریفات خود را می‌خواهد نشان دهد.

راهنمایی: برای استفاده در دستور hash بازیست از مسیر زیرنگاری شده. مسیر اصلی از hash استفاده از سیم خواه  
از دسترسی هار hash را درست کرد و این آن به اینکه توان بیشتر (getting x from  $y = h(x)$ )  
آناتر بخوبی که بخواهیم نمایند. مسیر اصلی از hash استفاده از مسیر شروع از مسیر شروع در دسترسی  
دسترسی از hash معرفی شده است. ولذا برای اینکه این استفاده را بخواهیم داشت، مسیر اصلی از  
دسترسی از hash معرفی شده است. ولذا برای اینکه این استفاده را بخواهیم داشت، مسیر اصلی از  
دسترسی از hash معرفی شده است. ولذا برای اینکه این استفاده را بخواهیم داشت، مسیر اصلی از

hash(choice,r)  $\rightarrow$  دش (ریل چنگ)

$\gamma = \text{random}$

```

r ← randomGenerator
m = choice concat r
send Hash(m)

```

طبل سیریز Verify میں اسکا مکار ہے جو کہ اسکا بھار دار ہے۔ تاریخ تکمیل را ایکٹھی کر لے، وہی مکار ہے

- ① ✓ by preImage Resistance
  - ② ✓ by using random Number (breaking the limited choice Number) + PIR
  - ③ ✓ by second PreImage Resistance )

توجه: الگوریتم ونوم سود، کمپیوئر است - ساده hash هر سه انتها - رامزد خود را باشد، شاهد برداشتن باید.

## سؤال ۱:

با توجه به اگر  $d, e$  صفا وارد  $\varphi(N)$  باشند و  $d \in \text{mod } \varphi(N)$  باشد آنگاه  $d^e \equiv 1 \pmod{\varphi(N)}$  باشد. بنابراین  $d^e = 1$  در  $\mathbb{Z}/\varphi(N)\mathbb{Z}$  باشد و عبارت  $d^e \equiv 1 \pmod{\varphi(N)}$  باشد.

۱) سیاست‌گذارانی که راه حل بازرسی و محدودیت دلاریم بسیج نیرو است:

۱- میں عدالتیم و رادلیم سے مدد میں۔

- ۱۰ راهنمایی در مورد تراکم تراکم اورم:

$$K = cd - 1 = r^{t_r} \quad (t_r, r) = 1$$

۳- حال و تاکمین دیدهای طبق یادداشتگر نمود :

$$x_i = g^{k_{r^i}} \Rightarrow x_1 = g^{k_1}, x_r = g^{k_4}, \dots, x_t = g^{k_{r^t}} = r$$

$$1 \leq i \leq t$$

حل برازیل و مکالمه ای اینست و پس از آن:

$$q = \gcd(n-1, N)$$

الآن لا يرى أحدٌ في ذلك ملائكة، وإنما هو ملائكة (المرجع: ٢٧) ←

نَمَى، سَدَ بُرْدَةً إِسْلَامَ الْوَقْتِ وَكَلَّ وَسَعَهُ الْأَنَّةٌ - لِنَ دَادَهُ بَرَدَه

لَهُ أَنْ يُوْدِي بِكُلِّ مَا يَأْتِيهِمْ وَمُنْهِيٌّ بِسَوْلٍ بِكُلِّ سُبْرٍ نَّدَرَ

مکانیزم رفع محتوا

b) بیو محل‌گذاری تأثیر دهنده از بود public هرگفتنی، سوانح آن گفته را حب

٢- خدمة تجارية (public, private services)

نیز دست نموده و نایاب شد، حال درین کار

اگر شخص می‌داند private key را حفظ نماید، (QRN) را با public key بسازد

$$\text{privateKey} = (\text{publicKey})^{-1} \stackrel{q(N)}{\equiv} \text{privateKey} \quad \checkmark$$

لقد تم توضيح طريقة عمل المنشئ (C) (الذراع)  
حيث نعلم أن

$$d = e^{-1} \pmod{\varphi(N)} \quad \checkmark$$

we have  $N \rightarrow \varphi(N) \quad \checkmark$

we have  $e \quad \checkmark$

↳ public key  $\checkmark$

نمای اموزه که ایست جنین کل نسخه:

We have  $(Acc(S), K, \pi_K)$

calculate  $A = \pi_K^K \pmod{N}$  → if  $Acc(S) == A$  → verified  
else failed.

(b) بد اموزه هر دو درست و درست مکله مولکل داشتم و بازی  $\log(N)$  عدد است. این ساختار بر پایی این است که ارسال رکوردم. حال آنکه داده ها master - hash شوند اموزه هر دو درست شوند. ارسال غایب و این تعداد انتزاعی تغیر نمایم و تو و داریم و اینها باید مطابقت باشند.

(c) فرض کنید  $P_1, P_r$  از برام داشتند و  $P_1, P_r \notin S$  باشند. دوست اند و برام.

$$\begin{aligned} Acc(S) &\stackrel{?}{=} \pi_{P_1}^{P_1} \\ Acc(S) &\stackrel{?}{=} \pi_{P_r}^{P_r} \end{aligned} \quad \text{imagine } P_1, P_r \notin S \text{ but we tell}$$

$S = \{P_1, P_r, \dots, P_n\}$

$$\pi_{P_1 P_r} = g^{P_1 P_r \dots P_n} \pmod{N}$$

$$\Rightarrow \pi_{P_1 P_2}^{P_1 P_r} = (g^{P_1 P_r \dots P_n})^{P_1 P_r} \pmod{N} = g^{P_1 P_2 P_r \dots P_n} \pmod{N} = Acc(S) \quad \checkmark$$

so  $P_1, P_r \in S$ ,  $P_1, P_r$  considered not to be in  $S$  but we conclude that  $P_1, P_r \in S$

$P_1, P_r$  از برام داشتند و  $P_1, P_r \notin S$  باشند و  $S$  را تراویم ایشان را در  $S$  داشتند و  $P_1, P_r \in S$  باشند.

Consider  $x \notin S$

$$\Rightarrow (x, \prod_{i=1}^n s_i) = 1 \quad \underset{\exists a, b}{\Rightarrow} \quad ax + b \prod_{i=1}^n s_i = 1$$

حال بار ایت اور ملکیت و جنینی دار ایتم می ہیں:

$$(Acc(s))^b (g^a)^x \stackrel{?}{=} \left( g^{\prod_{i=1}^n s_i} \right)^b g^{ax} \stackrel{?}{=} g^{ax + b \prod_{i=1}^n s_i}$$

$$\stackrel{?}{=} g$$

لنا آئے حامل  $(Acc(s))^b (g^a)^x$  دریافت نہ برابر  $g$  نہ دارم کہ  $x$  عضو مجموعہ

نہست  
—

1) بارٹ خداوندی: جنینی عدالت

عده ملکیت و خاص ایتم میں  $S = \{s_1, s_2, \dots, s_m\}$  کا مجموعہ  $K = \{K_1, K_2, \dots, K_m\}$  میں قرار ہے

حال بارٹ زیرینہ میں:

$$S^K = \{ s_i \in S \mid s_i \notin K \}$$

aggregat proof (ایتم)

دراداہ خود بہت اور دیگر ایسے

single proof

$$\pi_{1C_{ag}} = g^{\prod_{s_i \in S^K} s_i}$$

$$g^K =$$

حال بارٹ اور ملکیت و خاص ایتم کا  $\{Acc(s), \prod_{i=1}^m K_i, \pi_{1C_{ag}}\}$  ایت

اور ملکیت و خاص ایتم کا  $\{s_i \mid 1 \leq i \leq m\}$  ایت

حال بارٹ اور ملکیت و خاص ایتم کا single proof

single Proofs

aggregation

$$(Acc(s), k_1, \pi_{k_1})$$

$$\left( \begin{array}{l} Acc(s) = Acc(s) \\ \text{for aggregation} \quad \text{for single proofs} \end{array} \right)$$

$$(Acc(s), k_r, \pi_{k_r})$$

:

$$(Acc(s), k_m, \pi_{k_m})$$

$$\left( \begin{array}{l} k = \prod_{i=1}^m k_i = k_1 \times k_r \times \dots \times k_m \\ \text{from single proofs} \end{array} \right)$$

for aggregation proof

$$\left( \pi_{k_{\text{ag}}} = \frac{\pi_{k_1} \times \pi_{k_r} \times \dots \times \pi_{k_m}}{(Acc(s))^{M-1}} \right)$$

$$(Acc(s), k_{\text{ag}}, \pi_{k_{\text{ag}}})$$

example:

$$\pi_{k_{\text{ag}}} = \frac{\pi_3 \times \pi_7}{Acc(s)} \quad / \quad k_{\text{ag}} = 3 \times 7 = 21$$

$$(Acc(s), 21, \pi_{k_{\text{ag}}}) \checkmark$$

$$s = k - xe$$

و

$$g^s = g^{k-xe} = g^k (g^x)^{-e}$$

روجنسنیه فیلی عبارت دارد از این

$$\Rightarrow g^s y^e = g^k$$

$$\text{بر} \quad e = H(r || m) \quad \xrightarrow{r=g^k} \quad e = H(g^k || m) = H(g^s y^e || m) \quad \text{OK}$$

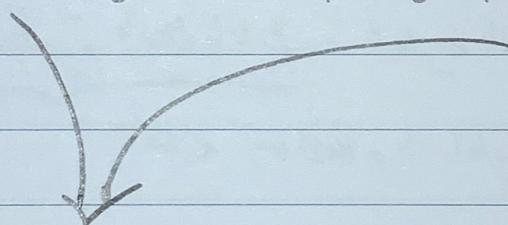
- ما  $s$  را درم نیز signature اسما

- و را درم زیرا برای مدل عناصر است (کمی)

- generator و  $y$  را درم نیز عرض می‌کنیم.

- سیم  $m$  را درم نیز.

- الگوریتم  $H$  هم خوب بود و آن را درم نیز.



لطفاً این عبارت را از این اطلاعات

برداشت نکردیم. اگر برایم بود یعنی اینها مابالی  
کس است که مایل عرض دارد است.

## سوال ۷

حاسه سوال می باشد که نسخه های دیگر طبق (خصوص این تراز) چنین اتفاق نمی تواند باشد.

$$S = K' * (h + r \cdot d) \pmod{n}$$

$$\Rightarrow kcs = h + r.d \pmod{n}$$

$$\Rightarrow S^{-1} = k * (h + r.d)^{-1} \pmod{n} \quad ①$$

$$\begin{aligned}
 hS^{-1}G + rS^{-1}D &\stackrel{\textcircled{1}}{=} h(K(h+r.d)^{-1})G + r(K(h+r.d)^{-1})D \\
 &= h(K(h+r.d)^{-1})G + r(K(h+r.d)^{-1})d.G \\
 &= K(h+r.d)^{-1} \underbrace{(h+r.d)G}_{\approx 1} \\
 &= KG = R
 \end{aligned}$$

get X coordinate( $R$ ) should  $r$

ما د رادیم ، لکن  $h = \text{Hash}(m)$  د رادیم . (جواب داریم .) (I)

①, ②  $\Rightarrow$  we have  $hs^{-1}G + rs^{-1}D \rightsquigarrow \Rightarrow$

لذا يرجى اعتماد المعايير المذكورة في المعيار

دانش‌های خود به آن رسم و حال آن را درست کنید و درسته اوریم و درسته را درینجا و داریم که اینجا درسته اوریم

if  $R_n = r \Rightarrow$  signature is valid.

$\neq r \Rightarrow$  invalid state.

Public Key =  $(G, q, g, h)$

: ① جملہ

لے اور سادھی تر میں دو

$$c_r = m \cdot s = m h^y$$

$$c_1 = g^y \Rightarrow c_1^x = g^{xy} = (g^x)^y = h^y$$

پس  $c_1^x = h^y$   
 $c_r = m h^y \quad | \Rightarrow m = c_r (c_1^x)^{-1}$

ذکر میں  $G, c_1, c_1^x$  مارک ✓



Description given  $(c_1, c_r) : m = c_r (c_1^x)^{-1} \quad \checkmark$

Plain Text