

Subject

۱

Date : Year:

Month:

Day:

## مبانی رایاسی امن

از زیبی: مبانی ترم

V مبانی ترم

۲-۳ سهیم و کوچیم

۴-۵ پروردگار

۱-۲ معالیت طاسی

۲۳ - ۲۵ ← بهترین سیزده دینه افلاطون لئن

امست → حافظت از هر چیز از سیندی در مقابل تهدیدات و مهادنی لئن تو نم مددی باشندیا  
دارایی

غمیر محمدی → برای مقنای سایبری هم همینه → سهیمین دارایی توی مقنای سایبری داده است

امست داده = حافظت از داده در مقابل تهدیدات و مهادنی لئن تو نم مددی یا غمیر محمدی

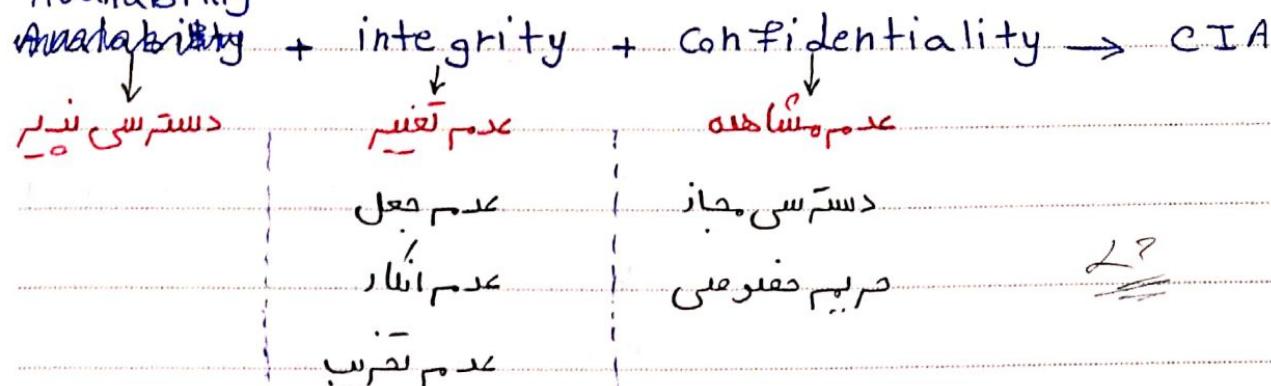
باشد

از داده حافظت یعنی چی؟ → صفت بعدی حدول میگیرد

Subject

Date : Year: Month: Day:

## Availability



5

لئن لئن ← این سه آنچه مطلع هم امیست داده رومی سازه ← CIA

لئن برای داده این سه ایجاد کنی "برتره ارلشی" توسف ساز دارا می باشد  
چه کسی؟ ← درس ما راجع به این چه کسی است

10

Good Guys



A → Alice ← بیوی از این استفاده می کنند

B → Bob

Bad Guys



مجرم داده مفعال نهایتی می نمایند

active میانات ←

Charlie

passive میانات

Dave

لئن سه ها را دست و کاری نمی کنند

میں حاسوس افتخارها

15

Alice's online Bank = AOB

لئن ← بانک اینلاین داره به اسیم Alice

Trudy باید بجهه چیزهایی توبه لسد ، الینه جیز Trudy Bob و Alice ← AOB

parsian

Subject

Date : Year Month Day:

هدف هست Trudy  $\leftarrow A \rightarrow B$   
کسی تواند بسته باید باشیم

لهم تواند بسته باید باشیم

Trudy کی می‌خواهد تری سسیتی؟  $\leftarrow$  جدول مفعہ 2

سر مفصل ها:

✓ cryptography  $\rightarrow$  crypto basics, symmetric key crypto, signature  $\leftarrow$  public key crypto, hash functions

✓ Access Control  $\rightarrow$  Authentication : passwords  
 $\hookrightarrow$  Authorization

✓ protocols  $\rightarrow$  1- simple protocols 2- real world security protocols

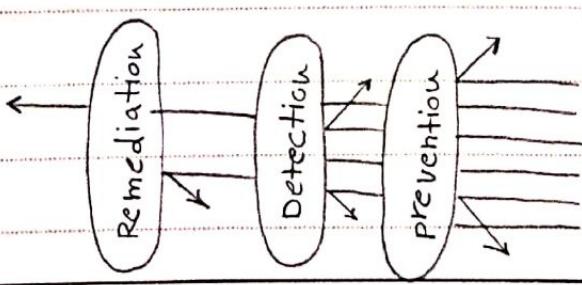
✓ Software  $\rightarrow$  1- vulnerabilities 2- Malware

\* 3 نادویم داریم برای این سازوگارهای امنیتی رایج داشتیم:

1- prevention  $\leftarrow$  سلیمانی

2- Detection

20 3- Remediation  $\rightarrow$  درمان  $\leftarrow$  معنی مادر اتفاق افتاد چیزی را این مله را درمان کنیم



parsian

1- دفاع در حقیق  $\leftarrow$  میزان این زاید سنت

2- به امنیت 100% همچو  
و متناسب باشیم

متقابل به درجه حساسیت لئے  
3 بایسی آزمایش را ممکن خنثی کن  
prevention

\* حِلْمٌ هُوَ زَيْنُ الْعِزَّةِ مَنْكَ أَمْسَى سَلَّمَهُ، أَمْسَى مَا دَرَصَدَنَا إِنَّمَا

۱- اسیسٹنڈنٹری مددیں ← حلہ مدد داری ← لعنی

۵- ارتباط ایزارهای تهاجمی  $\leftarrow$  عدم ساختن املفنا در سطح آشی و مردم

### ۳- تلاس بداعم راهنمای اقتصادی

لیعنی نفعاً و هر مال سبکه میل تراویث اینسا را باید می‌لیرن و میل اون عمل می‌لرسد

۱۰ نلتھ بھرداری امینت طا لھیدھ است چرا؟ چون باید دو تماوازنہ بھردار لئیں  
        حد  
        حد

۱- امیت و عملکرد  $\rightarrow$  عملکرد اولویت داره و باعثی من سه وزن امیت لامبست لامبست حون برای من همه  
ادن نرم اقداره کارلنه (عملکرد)

۱۵ ۲- امیت و هزنه  $\leftrightarrow$  خسی از ملائمه های امیت هزنه بر است

### ۳- امراءن ادیسات

## ٤- اقراض معنی

لکس بـ تاری امـست طـ سـنـ هـمـ است



## Crypto

وکان  $\rightarrow$   $\leftarrow$  تعریف وارگان بود  $\rightarrow$

نکته  $\rightarrow$  تنا هیزی Trudy  $\rightarrow$  دون طبیعت است و یعنی هر امکان اکتو دانادار می دویند  $\rightarrow$   
 لئے سی اصل اینوی کلمه هم لاتنا هیزی  $\rightarrow$  Trudy  $\rightarrow$  دون طبیعت

نه  $\rightarrow$  طبع مقام ها خلیق سایر نشست از نظر ?

10 ? داده Ciphertext  $\rightarrow$  Trudy  $\rightarrow$  5

\* کتاب سیفر  $\rightarrow$  آغاز  $\rightarrow$  دایره:

1  $\rightarrow$  سیف  $\rightarrow$  هزار  $\rightarrow$  2

15 17  $\rightarrow$  سایر ماتماتیک  $\rightarrow$  یونان کدوم سده و سی و سی هزار میلادی

22  $\rightarrow$  این تمدن از نایاب است  $\rightarrow$  an Time pad  $\rightarrow$  18

کدام سوتین اسفادس مال سوری بود  $\rightarrow$  حراس استفاده می شد?  
 چون طبیعتی تونه بصر رنگ  
 این لغرسن



stream cipher → security ↓ practical ↑

OTP لکچر از

confusion ارتعاش

block cipher → diffusion confusion

4F پی داست ← 38 ← A5/1 ← سفت (جیسته داست) ← همچنین

42 ← سفت (جیسته های بولی) سخت اتاری مناسب همچنین

10 ← چون اجرای حین تایپ وس داریم سین می دیم لری نرم افزار

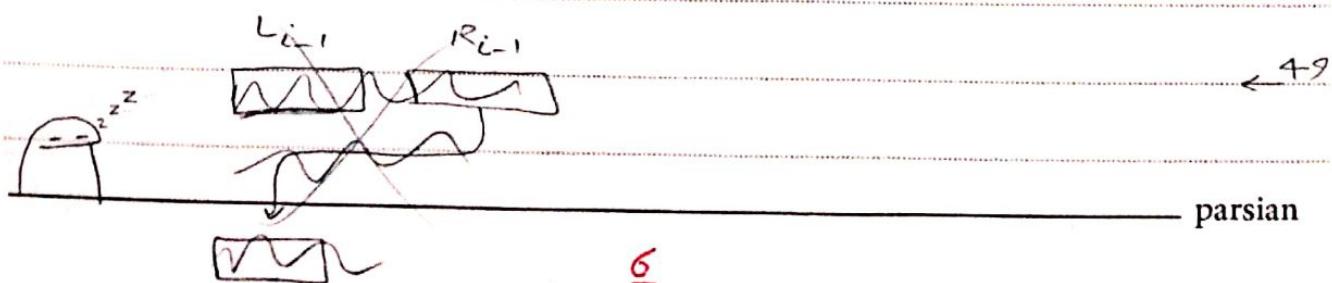
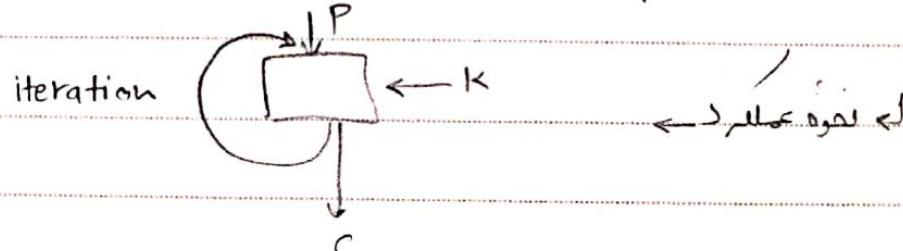
256

256 ← 43 حونه داریم توی هر حونه می دونه از مغفرتا 255 باشی

ملمه A5/1 پی داست می ده دلیل RCT بیانی می ده

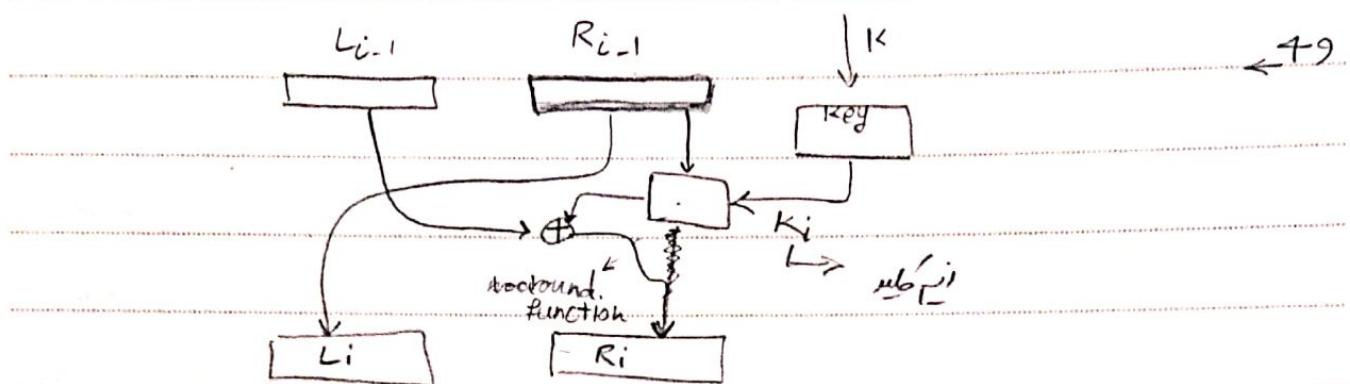
256 باشی اول را در می دیزیم چه (اتری)

بلوک را می لیریم یعنی بلوکی به مامی ده



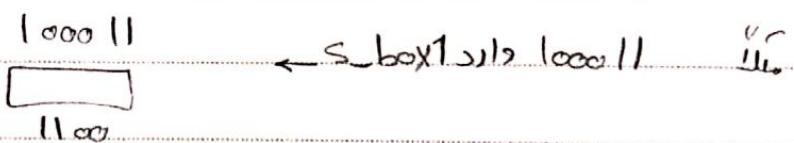
Subject

Date : Year: Month: Day:

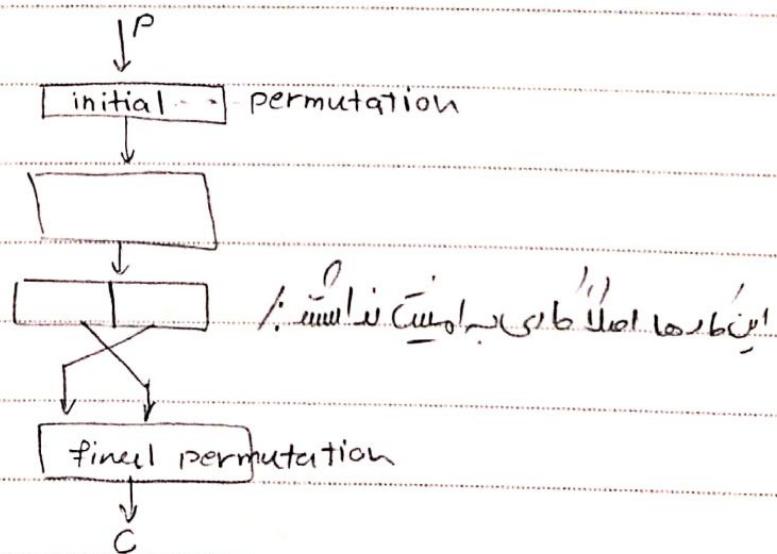


پایه س باخ  $L_i \leftarrow S\text{-box} \leftarrow \text{rule}$

10



15



20



parsian

5

Cauê Lé DES 191 140 ← 1997

st DES Ciclew 56 ← 1998

μ 11 Calw 23 ← 1999 5

النوع DES

از مبارکه استاد ۶۴

Triple DES  $\leftarrow$  DES  $\oplus$  DES  $\oplus$  DES

```

graph TD
    P((P)) -- "K1" --> X((X))
    X -- "K2" --> C((C))

```

لوي راند

69 - توجه مفهوم حیلچشم از مورد نظر

## ۱۱۰ - دو زندادی

### Mix Column



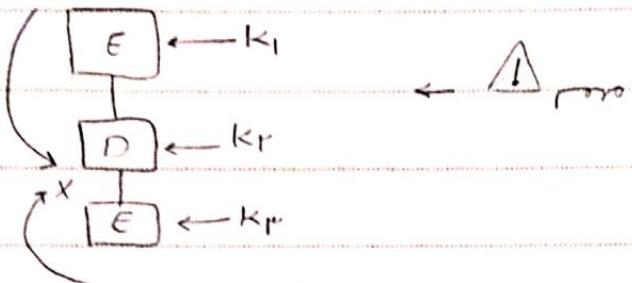
Subject \*

Date : Year: Month: Day:

نامہ را نصیر بچھوں انا زہل پیاز داره وردی با ملید ۲۰ خورشیدی

6

5



۸۵ ← IV می فرستی

10

کام کم Trudy یعنی از بیان مامن ای رو برداره چو کیا همی خراب می شے؟ دو تابلا لس

خراب می شے

15

نامہ یعنی دو تابلا plaintext برابر دو تابلا ciphertext بینان بیمانی ده

88 ← ایضاً IV را داریم رمزی لسی

20

۱۰۷ ← یعنی اون اسنه بیت عدد مون یعنی  $5+8$  می فرستی

کیمی Trudy سلسلت این روز سفته



parsian

7

$$\tilde{n} = \underline{p} \underline{q}$$

← RSA

جز اول همین بیانه

جنتا درس معرفت برای  $\tilde{n}$  اعداد صحیح داریم:1- Quadratic sieve  $\rightarrow O(e^{68})$  non  $O(e^{28})$ 

$$\hookrightarrow e^{68} = 3 \cdot 40 \dots \times 10^{29}$$

2- Elliptic curve factoring algorithm  $\rightarrow O(e^{65})$ 3- number Field sieve  $\rightarrow O(e^{60})$ پیمانه  $n$  را باقی بگذارید  $\leftarrow q, p$   $\leftarrow$  اول باید باشد

$$n \rightarrow \mathbb{Z}_n = \{0, \dots, n-1\}$$

عنصر که  $a$  و  $b$  باشند اول عدد نسبت بین اول اندبرای  $a, b$  معمولی  $\gcd(a, b) = 1$   $\leftarrow a, b = \text{coprime}$   
اویل اند

$$\tilde{\mathbb{Z}}_n^* \subseteq \mathbb{Z}_n \xrightarrow[n=10]{\text{def}} \mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$$

$$\hookrightarrow \phi(10) = 4$$

$$\hookrightarrow |\mathbb{Z}_n^*| = \phi(n) \leftarrow \mathbb{Z}_n^*$$

که این اول اعدادی که نسبت به  $n$  اول اند  $\rightarrow$  جموعه مخصوص یافته مانده های پیمانه  $n$  است

parsian

Subject

Date : Year: Month: Day:

$$\gcd(p, q) = 1 \quad \leftarrow \text{أكبر أول باسیت بین p و q} \quad 9$$

$$n = pq \Rightarrow \phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1) \quad \leftarrow \text{حقیقتی است}$$

$$5 \quad \phi(p) = p-1, \quad \phi(q) = q-1 \quad \leftarrow \begin{matrix} \text{أول باسیت بین p و q} \\ \text{لئے انہیں حقیقتی است} \end{matrix}$$

$$\rightarrow \mathbb{Z}_p^* = \{1, \dots, p-1\}$$

$$10 \quad \underbrace{m^x}_{m^e} \mod n = m^{\phi(n)} \mod n$$

$$ed = 1 \mod \phi(n) \quad aa^{-1} = 1 \mod n$$

این حقیقتی است

$$15 \quad \gcd(a, n) = 1 \quad \leftarrow \text{أول باسیت بین n و a} \quad 9$$
$$\rightarrow a^{\phi(n)} = 1 \mod n$$
$$\rightarrow a^{-1} = a^{\phi(n)-1} \mod n$$

$$\text{Sub} \rightarrow \phi a^{-1} \mod n = a^{\phi(n)} \mod n = \phi a \mod n \quad \phi(n)^{-1}$$

$$20 \rightarrow a^{-1} \mod n = a^{\phi(n)-1} \mod n$$

integer ہے؟ ریاضی میں ایسا ہے RSA.

فی بوده  $\phi(n)$  توان پرینگ (n) می باشد  $n = pq$   $\rightarrow$  Trudy از

$$x^y \rightarrow x^{2y} = (x^y)^2 \rightarrow \text{double or square}$$

$$x^y \rightarrow x^{y+1} = x \cdot x^y$$

← 112. 5

$$c_1 = m_1^3 \bmod n_1$$

$$c_1 = x \bmod n_1$$

← 113.

$$c_2 = m_2^3 \bmod n_2$$

$$c_2 = x \bmod n_2$$

$$\tilde{c}_3 = m_3^3 \bmod n_3$$

$$m = ?$$

$$c_n = x \bmod n_n$$

$$\tilde{x} = ?$$



جواب  
x

10

15

20

$$1 < d_A < p-1 \quad \text{Alice} \quad e_A = g^{d_A} \bmod p$$

$$1 < d_B < p-1 \quad \text{Bob} \quad e_B = g^{d_B} \bmod p$$

رسی داده کی

$$c_1 = g^{k_1} \bmod p \quad c_1, c_r \rightarrow m=?$$

$$c_r = m \times e_B^{k_1} \bmod p$$

 $c_1$ 

وابس

15

✓ ✓  
 سوالات  
 / /

20

9

Start

133

لے امر لسی طبیعی مخصوص لرفت باید اعلام کرنے والا، بعد از اون سفارشی یا حینی داد

5 ترکیبی طریق من نیست

144

Trudy  $\longrightarrow$  Bob

(Alice,  $e_T$ ), s

$$\{ [ (Alice, e_A) ]_{CA} \}_{CA}$$

s

$$\rightarrow \{ [ (Trudy, e_T) ]_{CA} \}_{CA}$$

10

10

pre-birthday problem  $\leftarrow$  چهل هفته  $\leftarrow$  158 سیمی؟

15

$$\hookrightarrow \left( \frac{364}{365} \right) \times \left( \frac{364}{365} \right) \times \dots \times \left( \frac{364}{365} \right) = \left( \frac{364}{365} \right)^n$$

لے تئی سی افراد نیستند ایکھاں (از زخماں) داریم لہوئی خواہیں

$$1 - \left( \frac{364}{365} \right)^n$$

20

کالج ریاضیاتی

خطای خود و جو دنیاد برای یونیورسیٹی خطای غیر عجمی است  
parsian

Subject

Date : Year: Month: Day:

MD5

1991

لـ اسـهـانـدـارـدـهـبـودـ

بـهـمـدـیـ اـنـاـحـهـ



SHA - 1

1995

NIST

attack

theoretical 2007  
practical 2017

5

SHA - 2

2001

NIST

SHA - 3 →

AES مـلـعـقـابـ مـسـالـهـ بـرـزـارـ

10

→ 2007 → غـرـاخـوـسـ سـدـ

→ 2008 → ۴K تـاـراـثـ دـادـد~

→ 2010 → سـتـاـهـاـيـ سـدـ

→ 2012 → لـوسـ الـرـوـلـيـمـ Keccak

SHA - 3 ← بـرـزـهـ سـدـ

15

→ 2015 → اـسـهـانـدـارـدـهـ

وـرـدـیـ دـفـوـهـ اـسـتـ

Keccak

وـلـوـيـ ضـرـوـجـ هـاـرـايـ

112

3DES ← 224

128

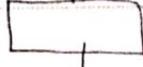
AES ← 256

192

AES ← 337

256

AES ← 512



→

سـعـاحـمـتـيـ اـنـ

3DES

→

u

→

u

سـفـارـاسـفـنـيـ دـارـهـ <-- لـعـنـ حـذـبـ مـنـ لـنـ عـسـ مـلـهـ  
اـنـ خـرـوـجـيـ هـاـيـ دـارـهـ <-- SHA - 3  
سـفـارـاسـفـنـيـ دـارـهـ <-- SHA - 3  
وـلـوـيـ فـسـابـ سـفـارـاسـفـنـيـ دـارـهـ <-- SHA - 3

absorbing phase

SHA - 3 sponge construction

squeezing " parsian

SHA-3 ل = 1400  $\sum L = 400$

Subject

Date : Year: Month: Day: / /

Kerck

state  $\rightarrow 2^L$   $L = 0, \dots, 4$   $\leftarrow$  مجموعه دارای  $L$  اتمت های

$b = 25 \times 2^L \Rightarrow b_L = \{25, 50, 100, \dots, 1600\}$

$L = 0, 1, 2, \dots, 6$   $b = 1600$

SHA = 3

bounds  $\rightarrow h_r = 12 + 2L \rightarrow SHA-3 : 24 \rightarrow SHA-3$  دوری

نقداً تجربی

مقدار output  $b$  rate capacity  $c$   $b = r + c$

227 1600 1152 448

256 ~ 1038 512  $\Rightarrow$  این مدل

384 ~ 832 768  $\rightarrow$  SHA-3 مدل 10

512 ~ 576 1024

rate یعنی ورودی که اون پر باشد

با سه ساختار rate  $r$  باشند

با هم فرقی اندیشیدم به 3 SHA-3

عملکرد

نمودار ضرفت با سه حزمی  $r$  و  $c$  و  $b$  ( squeezing )

نمودار ضرفت با سه حزمی  $r$  و  $c$  و  $b$  ( squeezing )

استخراج داد

SHA-3

توی تابع داریم که  $f$  بناشی داشت  $\rightarrow$  Kerck

از نوع ای

\*

input  $\rightarrow f \rightarrow$  output

1400 bit

1400 طاس واسه

دروی دادیم

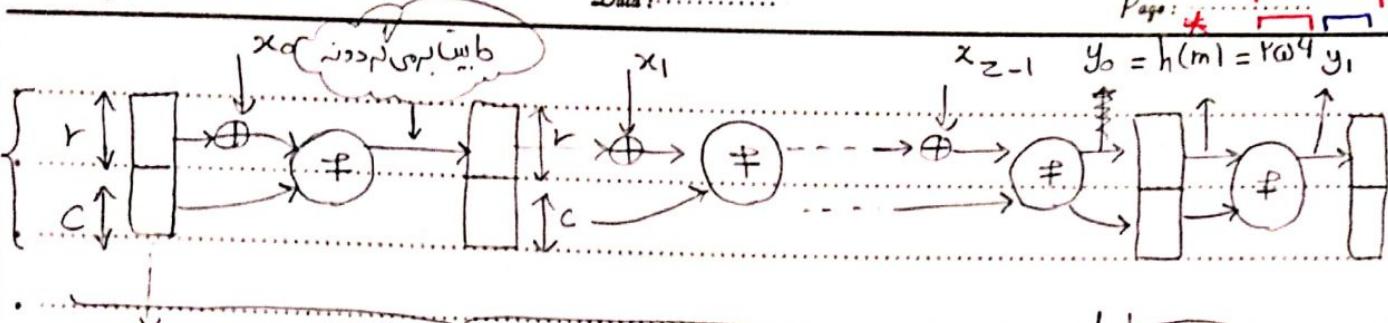
از این 1400 بعنوان

ضدی جایلست لف

لطفاً

دو تابع  $\rightarrow$  ( f ) است یعنی ملا داریه و ملا جیگسون  
بنی سه ساره

parsian



جودی را تحسین کنید.

Absorbing

حیرتکار اور مسلسل

squeezing

لهمه هر برآون حیری له مخفی است. له توی این مازدختها حذب می شوند بعد از این.

بسیار

کمال است یعنی صراحت و بی عیان

$$m + pad = x_1 - x_0$$

بالاتر است

حروفی از نیز نیز دوستیم

سامم

بله یعنی این حیری له الله صراحته بعوستیم یا امضا للهیم به عیان هس این ۲۰۰۴ سس است \* یعنی

بسیار سوین فرستیم یعنی بقیه ۲۰۰۸۸ سس و مسیحیت و مسیحیت و مسیحیت و مسیحیت

حیرن ال رهیل فرستیم بفرستیم و فرستیم بفرستیم بفرستیم بفرستیم

۱۵

فرازهایم حل و تحلیل سه اسماں: ز خ پ ر آ

این دنایا همراه اهل و مسلمانه توی این مراحل

بله از طبقتی بیست سی اس سس

این دنایا همراه اهل و مسلمانه توی این مراحل

برایم فرستیم

این دنایا همراه اهل و مسلمانه توی این مراحل

$$y_0 = \frac{c}{r} \cdot bit = h(m)$$

این دنایا همراه اهل و مسلمانه توی این مراحل

بیست از سی بروم دادیم که

دانیه اینجا می سه بوداصن بفرستیم بفرستیم

بیست از سی سه (۲۰۰۴) h

نسلیکے نتائج این ۳ نا مرحلہ ۔ توکی ۳۔ H.A. ۲۴ دور داریم یعنی ماترنس وارد میں وجہ

این ۳ نا مرحلہ ۲۴ بار دلوں ایضاً میں خروجی ماترنس مالدہ

و الگی عدد راندھائی تو داریم زیادہ ولی باز پڑھ بولیں

مزکیے مالز میسری ..... xor ..... and ..... سعف ..... اس قادہ میں لفظ میں Keccak سیستم سریع

کیا!

فلٹرے ۔ درای ایسے لفڑی بلطفی لفڑی لفڑی لفڑی فرستیم ۱۔ راہیں از سی بھی فرستیم

۲۔ ازادن سی تو داریم دلسے rate تعداد

حدیقی رامی فرستیم تو بستی دارہ بدھے

ویژی حجم ہس مان لفڑی ۳۔ one way ہر حدید ۴۔ بزرگتر باسہ از rate میں لفڑی

بود ۵۔ اسے ہمیں ہوئے ۶۔ رانی دیم سی فرستیم

نسلیکے عالدہ بروائیں چیری ۷۔ میں دھیں لے ۸۔ اما این ایمان را برات فراہم میں لفڑی

دلیل توکی سرمه ۔ ونگ زیک ہی state توبہ بیٹھیں لیم ۹۔

از این بیہمی کے ترکیب میں وحالت سب سی دندم دارہ میں تو نہ کلد تو لیل لند

12

M.G.K.

+ A  $\xrightarrow{M, h(K, M)}$  B  $\xleftarrow{\text{لبریاول سامانه بعد از مجموعه ذاریم}}$  HMAC

$$A \xrightarrow{u, h(M)} T \xrightarrow{u', h(M')} B$$

ملکیات سلیمانی داره خبایس بیخاسن از حسن اسناده لشیم داشت اینکه؟

• Trudy  $\leftarrow$  A  $\xrightarrow{M, h(M)}$  T  $\xrightarrow{M', h'(M')}$  B سالسو بالا ليس بغير يعني اوليس

جبن. اصل. لیر. سیف. لیمن. ترنسپریل. بی. هس. بلیم. کو...Trudy. دی. جیر. یانس. نی. آس. هون.

صوی، لین، اهل، Trudy، همه، حوزه، طلبدومن، دین، سیس، حق، مارلنهم؟

**جُنُق**.. أصل.. لـالجُنُق.. Tragedy.. طبع.. درسين.. دونه.. سبع.. تابع.. حسن.. لا.. طبع.. دار.. للنَّسْمِ.. +

بلطفه از دوستی خود را در میان اینها میگذراند. همان‌طور که می‌دانید، این اتفاقات از این‌جا شروع شده‌اند.

..... 20 ..... میں لئے سو... وہیں طلب دیر اہنا فریضیں لئیں گے جسیں۔ اخیر میں لئے

جـ... F. ← فرعون من لفظهم (B<sub>2</sub>, B<sub>1</sub>). = مـ باسـ. يعني Mـ باللـولـ حـارـسـ وـ.

$$h(M) = F(F(A_1, B_1), B_2) = F(h(B_1), B_2)$$

از بلوک اول سکریومن من لغتیم و همی ملول هایی نعدی. بسیان افغانستان مملکت

$$\mu' = (B_1, B_2, B_3)$$

فرهن من لشیم

$$\xrightarrow{h} h(\mu') = F(h(\mu), B_3) = F((F(A, B_1), B_2), B_3)$$

دلیل ایجادی فرستادن درست نسیت حون Trudy من تونه یه طاری لند ← Trudy بلدن

حدو لشن طرد توست بیام ایجاد لند و هسن هم بفرسلن

$$A \xrightarrow{\mu, h(K, M)} T \xrightarrow{h(K, M')} = F(h(K, M), X) \xrightarrow{M' = M, X} B$$

10 هسن طرد دار سازه ← Trudy من بعنده هن حافظه  $M' = M, X$  بسانده ← Trudy.

حدودی را تهیا می‌کنم آلسن افنا فله

15. حالات بعدی ← اول  $M$  باشید و بعد  $K$  ← سالش این حالات سخت از حالات قبل است

ایضاً فرن من لشیم از هسن غایلشن Collision من دو شیر سے یعنی  $M$  و  $M'$  می‌گردیم که

الله مطلع داشیم که سرانجام همه چنین هنسی Collision داده نایاب شدیم

20 لے احتمال دموع این لہمہ لست بیوه  $h(K, M) = h(M)$

آن دلیل ایجادی هنسی تراویق نمودند لے بر اسی collision وجود دارد پس ایضاً Trudy

$$A \xrightarrow{\mu, h(K, M)} T \xrightarrow{M', h(\mu, K)} B$$

$$h(\mu, K) = F(h(\mu), K)$$

25

$$h(M', K) = F(h(M'), K) = F(h(M), K)$$

حالات ایسوس ایمیل

pad باید مطابق با M باشد. یعنی  $h(M \oplus pad) = h(M) \oplus pad$

5

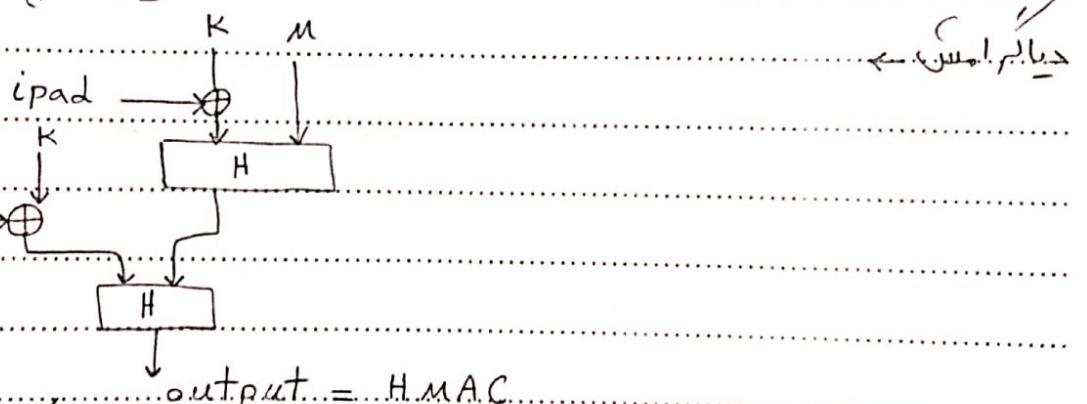
$iPad = \text{0x39}$  }  $\Rightarrow$  همین کار را می‌کند. B

$opad = \text{0x5C}$  }  $\Rightarrow$  همین کار را می‌کند. M

$$HMAC(M, K) = H(K^+ \oplus opad, H(K^+ \oplus iPad, M))$$

لے یعنی  $K^+ \oplus opad$  با صفت تابعیت B داشته است.

6



این پرآچار کو جاسه جیبی داشتیم. توی HMAC نداریم سه بخواهیم کرد این مطلب ایم

7

نه که همین دو هم می‌زنیم. چیز خوبی تو همیله ره

لے خوبی سریع بدهیم. جوابها من حمیون. تقدیم ایسا همچنانی که حمیون از تعمیر محاسبانی

8

این بیام خوبی بزرگ باشیم. همین دو هم مقابل نادیمه. لم فناه سین اس. حمیون برایں تقدیم

9

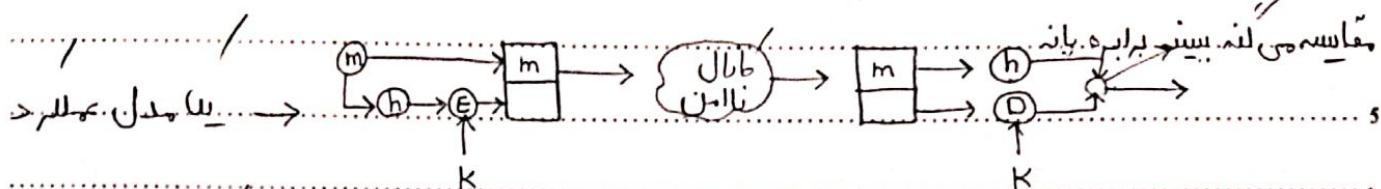
طاو محاسبان انجام نہیں دیجی

10

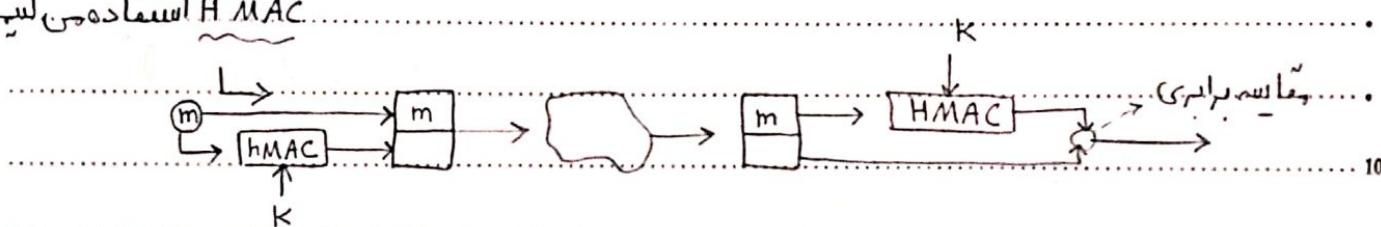
dp

از هسن لجاهها استاده می‌لشیم؟

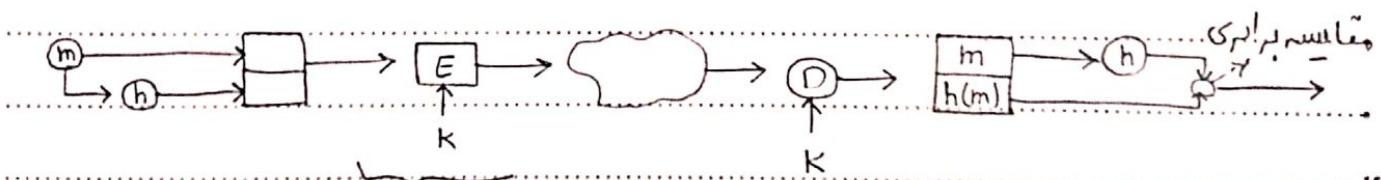
با این فاصله integrity حسنه می‌شود.



سلیمانی سی ان  
H MAC استاده می‌لشیم

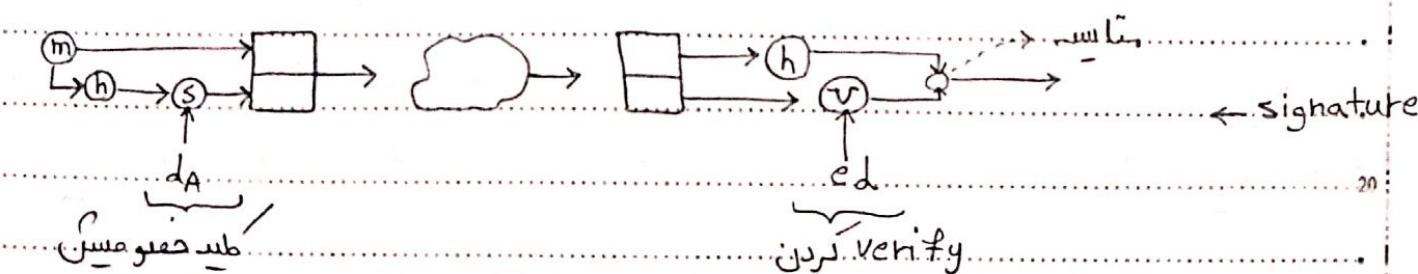


integrity + confidentiality



نکته ← اگر اینها استاده درجه همیلا طبیعی هستند، همان‌طوری همیلا هستند

طبیعی با هم مقایسه



13

steganography یا پنهان نهایی

هدفون: ... مخصوص نهیں ہیں اس لذت بدل میں اللہ ... ایضاً دنیا میں آزاد نہیں ...

سایروی ← آئس وابط تھی رسان ہستن وی سفیں نلہان میں داریم دجاجہ

من دم این آنا باہم یا من معادلہ لکھ ... یا قدرتی دارہ ... نایا من مسندی المعنی  
حقیقی اگر یا من دم سعدیا میں ... دبایب نلاسلف ... نسبی داشتے باشیں

لہجے تھی حمیں قعایق من خواہیم ایجاد ... برقرار رائیم ← هدفون: ارتباٹ لا جھی لشیم = cover

من لشیم ← قوتی ہیام دا جنمیں لشیم حالات سب ... لغتیم داریم ← بایس بید حالات سب ... لذت بدم داشتے

cryptographی ← plain text ... to ciphertext ... تونیا ... Trudy ... سے ...

سے حالت لشیم ... لذت بدم دا جنم دا جنم

هر من من لشیم ہیام دم سدھوں میں خواہیم وحود ارتباٹ لا جھی لشیم

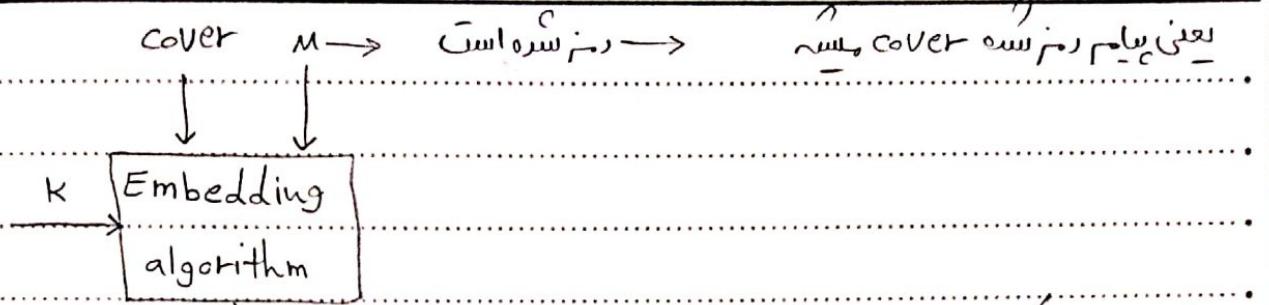
لوی ... steganography ... بے ہیام میں داریم

میں مقدیریہ ... لشیم دم سدھوں دھالت لشیم ... لذت بدم داریم

25

DANIAL

DP



وَهُمْ يَلْعَبُونَ مُنْتَهِيَّاً إِلَيْهِمْ لَوْلَىٰ ..... يَلْعَابُونَ اسْتَهَانُوا بِهِمْ تَوْسٌ يَحْقِنُ سَهَّدَ

• مکال ← السن دریو السن . معال ملیٹ زسیست من خود حاسوسی لنه وھڑوئی ھمھی لئے دعہ  
و مال

حالاً... حی باس؟  
..... *Cave!*  
لری مایل پش مجبوری بایم راحاسای لیم فرض من لیم بایم هم بلسری او ه است میلا  
و خر فیض هم لری من ده زیاد نیست..... *Cave!*

۱۵.۱۱.۱۰.۲. ← بوئی مایل متنی حاصله از یکم ساخته است: بوئی مایل متنی از ترکیب همچو بله نفعه است. اسماً ۲.

.....  
.....

نلئے ہے۔ نوکس... رمز... سلنی یا... Cryptanalysis... وہی مارٹن... رائلسیم... لہیا جلد رائقور... سنبی...  
نام... راؤی... فرطاسن... بھائی... لد اسنس... لد خارج... از... محدودہ... سینداری... ما... بستا... \*

لست آورده باسیم یا بایهانی از plaintext را بدست آورده باسیم ولی تری.

.....steganalysis.....باید لیسم بروی این مایلی <sup>اکنون</sup>.....انفورمی سنتا.....یعنی تری.....steganalysis.....

وَلِمَا كُلَّ فَلَيْسَ بِلِهَانٍ مِنْ سَا... Cover.stego... يعني سَا... فَالِيْلَ حَامِلٌ لَتَوْسِيْعِيْمَيْسَت

ما به این توانی حساسیتی داشته باشیم این سیستم از حدود مقادیری دست نماییم...  
steganalysis

موقـلـوـدـه

ادامه \* ← البر فرض (س) داشت یعنی بـ دارند است پس صفت ← از قدر استداری نبـ عده دارم

ویر، از ارها و مانع های است. ل. و. س. war. deh. با اون حاصل است. را بحلل من کن و اون مقابل.

...L...stegahalysis...

سندھن، اسٹا۔ و مسلو لامن سہ۔ ملے۔ Wat. deh۔ سے۔ خود ان مرسادن فاین صریح بیاد مسلول امیرنہ

فابيل وليد بورن ← البر فريسم هاسبر دالسته طاري. لنييم مولن. جيليم خراب للبيه و خل

سے! عزیز! میں ابھی وہ مطالب صدوق تراویح دار! وہ آئندہ بھی ہے! داہم غنیمہ من فضل اللہ

..... ← قَوْنِي ← مَرْسَى ← الْمُلْك ← لَقَوْنِي ← حَالَ ← مَدْوِلَ ← حَسْبَ ← لَسْتَ ← اَنْعَرَ ← وَحْدَه ← C.A.V.E.R.....

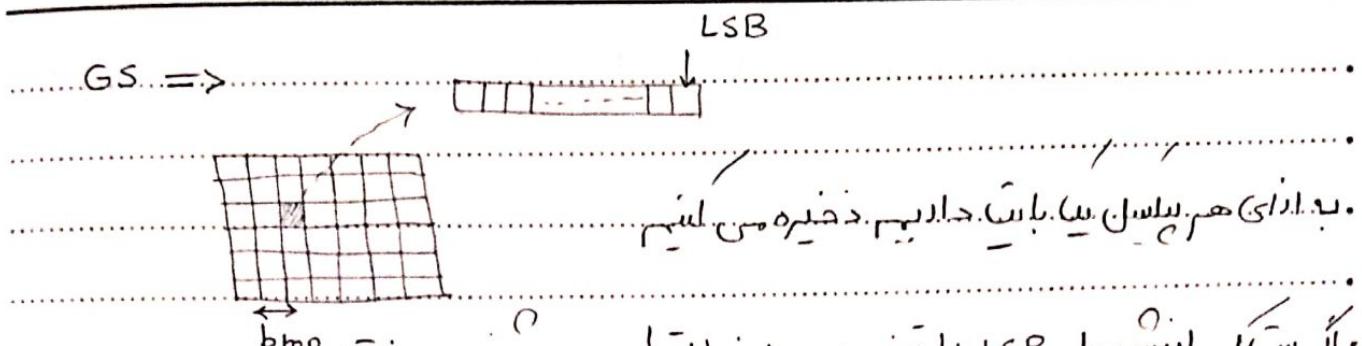
لقطیویز: سایم لوتوی پللسن ها. جا ساری لئیم. سے الیم. وی. کللس. د. استیم. ۰.۵.۰.۰۰۰۰

دادیم. یعنی معرفتی ما... مخصوصاً بسته است. تا زده این سلسلی دارد.

20.....

لطفاً... ای ساعت حال سریعاً با... GS... و... همچو عربی... GS... لغتی... و... ایم... هم برقراوه

نکاتی مبتداً در این روش است: RGB سیستم رنگی است.



۵. اگر سیستم ارسی یا LSB را تغییر بدهیم این از تغییر بعضی مسخون شست.

۶. انتساب پیکسل با استفاده از طبقه است. له حساسی بیوی اون پیکسل انجام می‌شود.

۷. اگر سیستم ارسی لجه حساسی حواسی لجه با LSB می‌بود تغییر می‌شود.

Cover LSB :

stego :

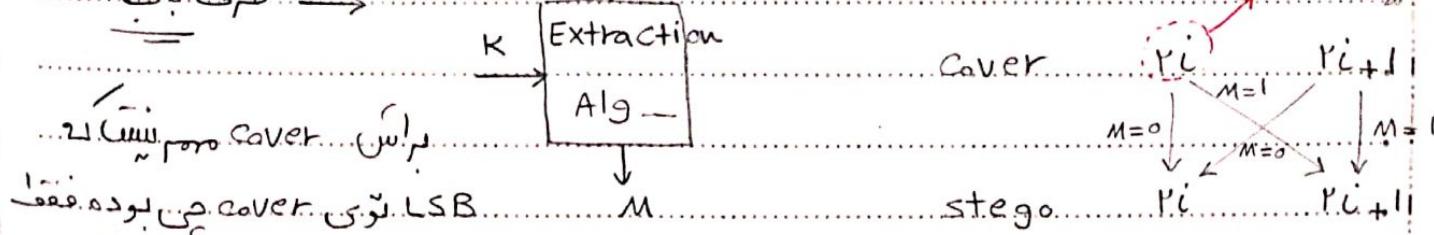
لهم از تغییر بعضی این قابل ساختن نشست.

۸. اولی بود مثلاً LSB اون پیکسل که انتساب سه صفر است دلی بیت هایم بله در این حالت

۹. اندیورس جاسین من لجه مثال می‌بودن را بالا بذیم باست صفر M

۱۰. نعم دلایل طبی دادارند یعنی هر ۳ فوت از دوستوی لوجه پیکسل یا مام حساسی سه

۱۱. این یعنی بیان لهی پیکسل انتساب سه ۲۶



۱۲. پس از این که LSB اون stego می‌بود

۱۳. نهایت از آنرا هم قرار گیری متن LSB های

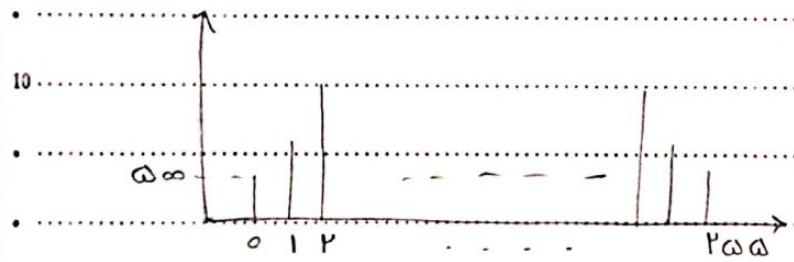
۱۴. غرمهول حرف های بیا

بداین روش که مادریم LSBR می‌لئیم replace باست. ساممی لئیم replacement.

\* LS.BR... مجبوری سلنے سے اپنے راحتی خلیٰ راستے کی مدد کیوں؟

حسینو لر لام بیل عذریم  $\rightarrow$  میلا از ... تا ... داریم. حسینو لر لام من سواره له میلا مقدار حضر.

لوبی لفکوییر چینیا راتلر اور سسہ. جلا۔ صافرے سے... مدد بار... = یعنی چند تا یک لسل دار یہم لہ پتدار عددی



اون. سلسلہ حاضری

بالسلفاجه از هستو برام ما... کارا من سلیمان

Diagram illustrating the flow of a fluid through a series of resistors. The flow starts at a 'Cover' boundary with a value of 1000. It passes through four resistors labeled  $R_{100}$ ,  $R_{200}$ ,  $R_{300}$ , and  $R_{400}$ . The total resistance is  $1000 + 200 + 300 + 400 = 1700$ . The final value is  $1000/(1000+1700) = 0.38$ .

**Stego** → **Stego**...**Stego**...**Stego**...**Vado**...**Vado**...**Vado**...**Vado**

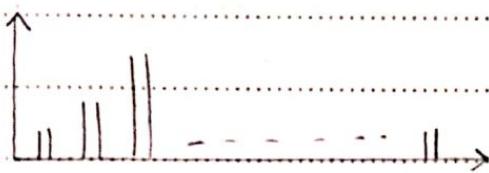
فرعنونین لئىنىم از ئەر قىتى تىقىلۇرىز بىغۇرۇ طاھىل استفادەمىن لئىنىم سەرچەن سەرچەن لە ئەسما ئەستىگىزىم

..... ١٢ .....  
من. لشیم. سه. آندهم. است. سو. اهتم. الا. اتفق. انصرف. ها. ملسو. لیت. حضر. و. لتفنا. دله. ع. مدل. علسن

<sup>25</sup> ... سالانی صفر است. این احتمال ۱/۳ می‌باشد که من حوا دخساری بسیار باشند. یا چه ای؟

جون سیام سبب نندو و برای تفسیر هم بجهن صورت

جی المفای توی من جبل افتاد؟ نا و اینکا هستوگرام دارن جفت حفنت من لش یعنی



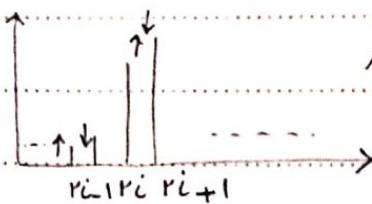
هستوگرام Stego S. هست

این به سرفی که توی نهادم لیلسل حاجاسازی  
ابنام سده باشه

نه ← حتی الرد صد حاجاسازی ها هم باشند و این هست لے USB هارو

سسایی من لنه کل دس سلیمان دلتا

← بارانی ایله چند درصد حاجاسازی لردیم نا و اینکا چقدر بزم  
حفت دس بالا استا → تردیم میشن و نک و ایکی چقدر از هم دور من شن و بجهن صورت



نه ← دس لے USB عدم تقارن داره جون از نک چیخ دقت لسم من سه یا به ایکی چیخ

جفت افتاده لنه سه

26 [cont.]

.14.

بله... همچنانکه سلسله هارا است سر همیز حاسانی ترس این خامنی دیده و بی از مطلع نمی شد. لفظیم ...

استفاده ناشیم. یعنی آن...  $m \times n$ . تابع  $f$  می‌تواند دارای  $m \times n$  تابعی باشد و محدود را هم حدود داشته باشد.

لشون و بحث تسبیل سلسلی به سلسلی سایم را حساسی لشونی می‌دانند اما اتفاقی من افتاد؟ هملاً هم دیدند...

حاسازی اینها ممکن است باشد. همچنان که در اینجا آورده شد، اینها ممکن است باشد.

سنت.....  
Steganalysis میاد برای فسیحت های مختلف لغت پر این تحلیل را انجام.

من ده. → حسستولر ام. طن. لقنویم. صفت. لین. الله ولی. هیستولر ام اون. ۱۰. صفت. من. سه. ←

..... ۱۵ میں از دلائلی لہ لحسن من لہیم و از طبیع استفاده من لہیم ھمین است

$\alpha \in [\underline{a}, \underline{1}]$  مقدار حساسیت کننده  $\alpha$  است.

طبل حاسواني لردیم  $\rightarrow$  ... لـ. يعني،  $\rightarrow$  حیث حاسواني

۲۰.....اکریباً رایمِ حاسانی بود. صدر اینا تغیر می‌شد؟

هـ ١٤٢٣ میونہ الہ باراہم حاسانی

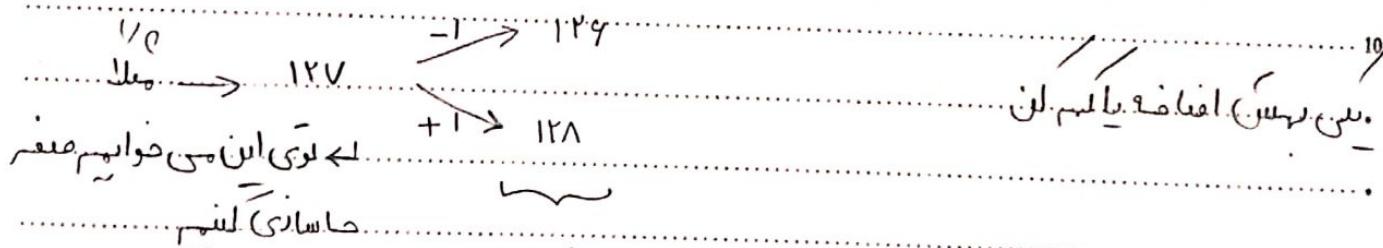
Mill  $\alpha$  DANIAI

سوال امتحانی ← h[i] + h[i+1]  
لے یعنی تعداد پسل هایی کو متداری کر است

لے آبیات لیں جو این آتا ہے مقدار مالی مونے از جو اینا بایس ریاست لیں  
لے یعنی برائی Cover جو حسی باو Stego میں مونے

رس LSBM ← مقابق لیم ارزش ترین سیستم

لے اگر M با SB میں است طاری ہے نہ اس سے بایس وہی الہ باہم یہی سیستم بعثوت رکھ دیں



توی 129 و 128 میں است اخراج سون توی Stego صفر است سیپن باز میں تو نیم توی Extraction

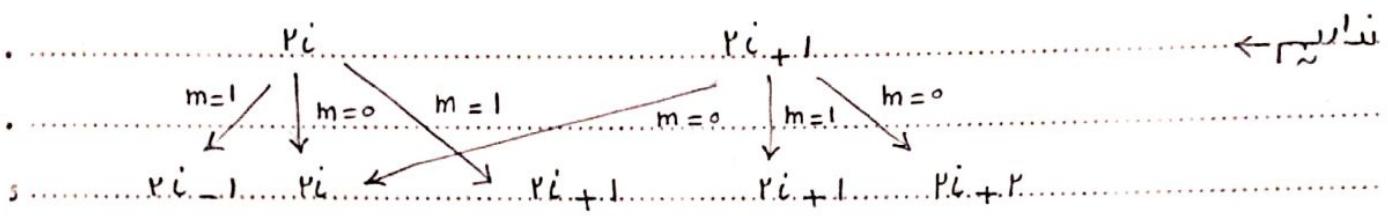
بعینام میا M بر سیم

$$\begin{array}{ccc} & \text{Cover} & \downarrow \text{LSB} \\ \text{y} & \rightarrow & \\ \text{z} & \rightarrow & x = \_ \end{array}$$

stego پسل توی است ←

$$y = \begin{cases} x & m_i = \text{LSB}_x \\ x \pm 1 & m_i \neq \text{LSB}_x \end{cases}$$

بلندی توی این لوس مسلسل عدم تقارن... LSB رفع سده  $\rightarrow$  یعنی توی این لوس ما عدم تقارن



بلندی  $\leftarrow$  آنچه نظری بحث LSBM می‌افتد correlation است. چون این می‌بینیم

از پیلسل های فتحه این اختلال به همین مقدار مسافت داشته باشد. توی کاپیلریون صفر

است بدین طوری این اختلال بسته از اینه که آنها بقروه است. از دو قسم صفر و یک باشند.

یعنی اندومینیتید

بلندی  $\leftarrow$  تمام لوس های پیشنهادی اس اس اس ان. LSBM است سه میاد جاهایی از قطبیم لذت گیری

می‌رسد. اینجاها را داسه جاسازی آنچه اینها می‌باشد

بلندی  $\leftarrow$  لوس هایی که برای سناسایی LSBM هستند. عمدتاً این بحث

طرحی لذت  $\leftarrow$  یعنی توی این حالت هیستو لرام چفته بین لذت و لذت لذت

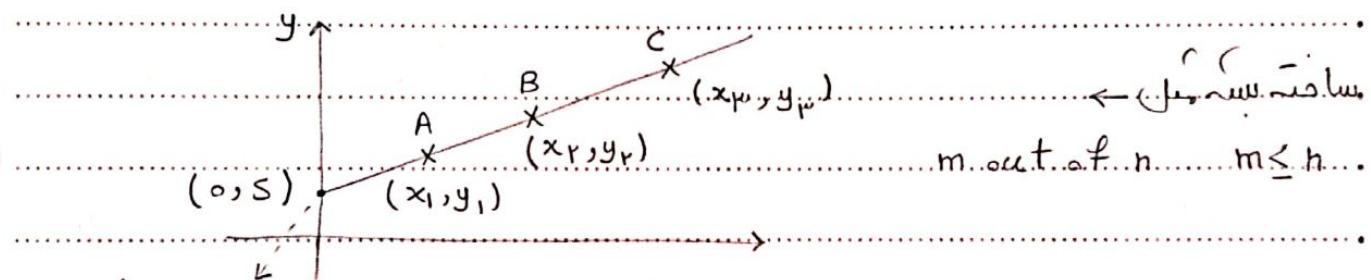
یعنی اینجاها لذتی هیستول ام ترنز، زرم جا پلی

هر از \* می‌دانیم در لذت این حالت تقارن خفته شده. ولی اخیراً پیلسل هارابیم

من المزبور

10  $\rightarrow$  secret sharing..  
سیم لردن راز مکلا برازی را بنی گیر، تقسیم نماید و اون گذاشت.

و لقرع عیناً باید باشد تا این راز ساخته شود و بی بعفونی و قضاهم نیاز نشست. لذا هبہ باشد تا رازه



محل برخورد با

هر ۲ قسم از ۳ قسم تو اند اون راز را  
محور یعنی میسک اون راز

ایجاد کنند

لے طبقه دسیں  $\rightarrow$  توی یعنی مکالمه هایی تقسیم

## 15. فعل ۲ Access control $\leftarrow$

لے راه ارتباط بین این دو بین مکالمه این واردین system بسرو و از صریق system بباب

در ارتباط باشد

Access control  $\rightarrow$  این که من خواهد داد وارد system بسی هد فسی این که از من ایغای

تسیم استفاده کند  $\rightarrow$  آتا سرگار داسه این مفهوم میگوییم

۲۱- آیا تو واقعاً همین که من کی هستی؟ ۲- حالات واردگردی به چه منابع تابعه میگردی  
جی تو نه دستگاه داشته باشی