به نام خدا

مبانی رایانش امن

دکتر موزرانی

تکلیف دوم

مهلت تحویل: جمعه هفدهم اردیبهشت - ساعت 23:59

1. در این سوال 5 متن رمزنگاری شده با الگوریتم سزار داده شده است. با استفاده از یکی از زبان های c/c++ و یا python متن اولیه آن‌ها را بدست آورید (راهنمایی: برای موارد iii,iv,v به جدول حروف ASCII توجه نمایید).

- اگر بخواهیم احتمال رخداد هر حرف در متن رمزنگاری شده را به ازای هر یک از 26 کلید ($\phi(i)$) برای مورد i,ii محاسبه کنیم، آیا همیشه بیشترین احتمال پاسخ مسئله است؟ آن را محاسبه کنید.

i) “HdxmjnjaoZsxcvibznzmqzm”

ii) “KfpjSjykqncfuutsUqfdXytwjhfzlmymnofhpnslBmfyxFuuxjxxntsx”

iii) “.4)/C+g-;)x'i1v0k:y'2=yz')xk6z';k+{:kF`OE”

iv) “9?4:Nw4>88G9?<K4CCBA#?4L&GBE864H:;G;<=46><A:*;4GFrCCF 8FF<BAFP”

v) “BH=CWPDEO;DKIASKNG;EO;=>KQP;?NULPKCN=LDU;=J@;GA U;I=J=CAIAJPhY”

پاسخ شما باید حاوی کد پاسخ سوال و پنج تصویر از خروجی آن که متن رمزگشایی شده در کنار کلید و احتمال آن (برای مورد i , ii) باشد.

.2

1- در صفحه 104 کتاب مثالی از یک متن رمز شده توسط الگوریتم رمز ویژنر ارائه شده و مراحل تحلیل این رمز به طور کامل شرح داده شده است. این مثال را مطالعه کرده و فرایند تحلیل رمز را به زبان خود شرح دهید.

2- در ادامه یک متن رمزنگاری شده با الگوریتم ویژنر داده شده است. سعی کنید با روشی که در بخش قبل مطالعه کرده‌اید، ابتدا اقدام به پیدا کردن طول کلید کنید سپس متن اولیه را پیدا کنید (برای بدست آوردن متن اولیه این امکان وجود دارد که از ابزارهای آنلاین یا آفلاین استفاده کنید).

"Llglv eji ouec jicmfrk xq vv hawcjgsarvyu efh ouec jicmfrk xq vv lgtgzlp.oi clv xzi qhvw olq xvgahg qyillgl ks ti jigixyn ii hawcjgsarvyu"

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

3- به سوالات زیر به طور مختصر پاسخ دهید.

- چرا با وجود رمزهای متقارن رمزهای نامتقارن ایجاد شدند؟
- کاربرد certificate در تبادل کلید چیست؟
- سه مورد از حملات به پروتکل های تبادل کلید را نام ببرید.
- در مورد معایب الگوریتم one_time_pad توضیح دهید.

4- با توجه به فایل PublicKey&CipherText ضمیمه شده، از چه نوع آسیب پذیری‌ای در الگوریتم RSA می‌توان برای شکستن آن و بدست آوردن کلید استفاده کرد؟

کدی به زبان python بنویسید که plaintext را بدست آورد (راهنمایی: می‌توانید از پکیج Crypto.Util استفاده کنید).

5- پروتکل‌های تبادل کلید جلسه زیر آسیب پذیر هستند.

- سه مورد از خصوصیات یک پروتکل امن برای تبادل کلید را نام ببرید.
- با توجه به بخش قبل معایب این پروتکل ها را نام ببرید.
- آیا امکان سوء استفاده از این پروتکل‌ها توسط Eve وجود دارد؟ در آن صورت، کامل توضیح دهید.
- راه حل پیشنهادی شما برای افزایش امنیت این پروتکل ها چیست؟

1)

$A \rightarrow T$: A, B

$T \rightarrow A$: $(K_S)\ K_{AT}$, $(K_S)\ K_{BT}$

$A \rightarrow B$: $(K_S)\ K_{BT}$, A

2)

A→ B: A, n_A

B→ A: n_B, B, $K_S \oplus$ MAC (n_B) K_{AB}, MAC (A, n_A) K_{AB}

A→B: A, MAC (A, n_B) K_{AB}

- MAC (M) K_{AB} : پیام M با کلید اصلی بین A و B، MAC گرفته می‌شود.

6- با بهره گیری از کتابخانه Openssl به سوالات زیر پاسخ دهید:

- با استفاده از کلید Private.key ضمیمه شده سعی کنید پارامترهای کلید (p ,q ,n ,e ,d) را استخراج کنید.
- یک متن رمز تحت عنوان cipher.txt در اختیار شما قرار گرفته است این متن رمز توسط base64 encode شده است پس از decode کردن آن، به کمک کلید Private.key موجود در فایل تکلیف متن را رمزگشایی کرده و plaintext مربوطه را بدست آورید.
- یک متن حاوی نام خود نوشته و به وسیله کلید خصوصی متن نوشته شده را امضا و با استفاده از base64 encode کرده و فایل نهایی را ضمیمه پاسخنامه خود نمایید.

7- متن زیر را توسط تابع هش HMAC با سایز بلوک‌های 64 بیتی و با استفاده از الگوریتم SHA-256 به کمک کلید داده شده رمز کنید(استفاده از کتابخانه آماده hmac ممنوع بوده و این تابع می بایست به طور کامل توسط شما پیاده سازی شود. نیازی به پیاده سازی SHA-256 نبوده و می توانید از توابع آماده کتابخانه hashlib استفاده نمایید).

Message = “Cryptography is the practice and study of techniques for secure communication” | Key = “security”

8- هدف از این سوال استفاده از PGP در سرویس ایمیل است. پاسخ سوال سوم تمرین را با استفاده از کلید عمومی PGP ضمیمه شده رمز کنید و به آدرس homeworks.secure@gmail.com ارسال نمایید.
- می‌توانید از افزونه Mailvelope استفاده نمایید.

(توجه: پاسخ سوال سوم را در سامانه نیز تحویل دهید.)

- سوالات زیر اختیاری هستند و می‌توانید برای دریافت نمره‌ی اضافه به آن‌ها پاسخ دهید.

- در مورد ساختار الگوریتم‌های twofish، serpent و MARS توضیح دهید.
- روش‌هایی برای افزایش امنیت الگوریتم ویژنر نام ببرید.
- علت استفاده از s_boxها در DES چیست؟ توضیح دهید که اگر s_boxها نباشند، چه حملاتی به DES می‌تواند وارد شود؟

لطفًا به نکات زیر توجه نمایید:

- در صورت وجود سوال و یا ابهام، می‌توانید به ایمیل‌های زیر پیام دهید:

Sara.br1378@gmail.com (سارا برادران)

ae.naderi@gmail.com (عاطفه نادری)

- فایل تکلیف را در سامانه تحویل دهید و به فرم name_stdnumber.zip باشد.
- پاسخ شما باید حاوی (پاسخ نهایی+ کد سوالات مشخص به همراه توضیحات کد) باشد.
- به تکالیف مشابه نمره ای تعلق نخواهد گرفت.
- تکالیف به ازای هر روز تاخیر، 10٪ از نمره آن کسر می‌گردد.

سلامت و موفق باشید.