Lab1

Atribuiți fiecărui termen definiția corespunzătoare. Definițiile au fost preluate din glosarul de termeni *NIST – Computer Security Resource Center* [1].

(A) Adversar	(1) O condiție care rezultă din stabilirea și menținerea măsurilor de protecție care permit unei organizații/sistem să își îndeplinească misiunea sau funcțiile critice, în ciuda riscurilor reprezentate de amenințări.
(B) Securitate	(2) Slăbiciune într-un sistem informațional, proceduri de securitate ale sistemului, controale interne sau implementare care ar fi putea fi exploatate sau declanșate de o sursă de amenințare.
(C) Risc	(3) O entitate (inclusiv un *insider*) care acționează rău intenționat pentru a compromite un sistem.
(D) Vulnerabilitate	(4) Capacitatea de a proteja / apăra spațiul cibernetic de atacuri cibernetice.
(E) Securitatea cibernetică	(5) O măsură a gradului în care o entitate este amenințată de o eventuală circumstanță sau eveniment.

Rezolvare:

I.

(A) -> 3

(B) -> 1

(C) -> 5

(D) -> 2

(E) -> 4

Lab2

2. *Sisteme de criptare istorice*

Citiți despre sistemele de criptare istorice și experimentați cu resursele disponibile online [1-2].

1. Alegeți un sistem istoric de criptare care folosește *metoda substituției*. Dați un exemplu de criptare și un exemplu de decriptare, explicând cum funcționează. Ce puteți spune despre securitatea sistemului de criptare? Ce tehnici de criptanaliză ați putea folosi pentru a sparge sistemul?
2. Alegeți un sistem istoric de criptare care folosește *metoda transpoziției*. Dați un exemplu de criptare și un exemplu de decriptare, explicând cum funcționează. Ce puteți spune despre securitatea sistemului de criptare? Ce tehnici de criptanaliză ați putea folosi pentru a sparge sistemul?

Ex 2 -> metoda de criptare cu substitutie -> substitution chiper -> se inlocuiesc literele cu alte litere existente in text (substitutie)

ex: cifrul lui Caesar foloseste metoda substitutiei -> fiecare litera din alfabet e inlocuita de succesoarea ei

ca sa decriptezi trebuie sa stii tabelul cu substitutiile folosite

Caesar -> The Caesar cipher (or Caesar code) is a monoalphabetic substitution cipher, where each letter is replaced by another letter located a little further in the alphabet (therefore shifted but always the same for given cipher message). The shift distance is chosen by a number called the offset, which can be right (A to B) or left (B to A).

criptare -> diferenta de 3 litere

decriptare -> cauti o litera care e predecesoare

ex criptare: Exqd yu vd pd xlw od Ornl

ex decriptare: Buna vr sa ma uit la Loki

Metoda Transpozitiei

ex The Rail Fence Cipher, The Latin Square

The Latin Square -> is an intriguing example of a transposition cipher. It is made up of a series of 5-letter words arranged in a square, found on the walls of Roman villas in Pompeii and Cirencester.

metoda de generare -> o matrice n x n. pe prima linie e cuvantul normal, pe urmatoaarea sunt literele mutate la dr cu o unitate, pe a treia cu doua unitati, pana cand se ajunge din nou la cuvantul inital

metoda de decriptare -> The resolution algorithm consists in noting, for each unfilled cell, the list of possible symbols respecting the rules (prohibition of 2 identical symbols on the same line or the same column), if only one symbol among the N is possible then fill in the cell with this symbol.

Lab3

1) Atribuiți fiecărui termen definiția corespunzătoare. Definițiile au fost preluate din glosarul de termeni *NIST – Computer Security Resource Center* [1].

A - 4 (A) Criptologie

B - 2 (B) Criptografie

C - 5 (C) Criptanaliză

D - 1 (D) Confdențialitate

E - 6 (E) Integritate

F – 3 (F) Disponibilitate

(1) Asigurarea că informațiile nu sunt dezvăluite entităților neautorizate.

(2) Disciplina care studiază principiile, mijloacele și metodele de transformare a datelor pentru a ascunde conținutul lor semantic, a preveni utilizarea lor neautorizată sau a preveni modificarea lor nedetectată.

(3) Asigurarea accesului și utilizării informațiilor în timp util și fiabil.

(4) Știința care se ocupă de criptanaliză și criptografie.

(5) Încercarea de a înfrânge protecția criptografice fără o cunoaștere inițială a cheii utilizate în furnizarea protecției.

(6) Protejarea împotriva modificării sau distrugerii necorespunzătoare a informațiilor.

3) Răspundeți cu adevărat sau fals:

1. Un adversar care are la dispoziție un timp infinit pentru criptanaliza unui sistem este un adversar PPT.
2. Un adversar PPT are dreptul de a „ghici” cheia.
3. Un adversar PPT are la dispoziție algoritmi exponențiali în timp.

1.F

2.A

3.F

4. *Funcții neglijabile*

Înțelegeți ce înseamnă o funcție *neglijabilă* vs. *ne-neglijabilă* (într-un parametru de securitate, dpdv al unui adversar PPT, etc.).

Care dintre următoarele funcții sunt neglijabile în parametrul de securitate n, având în vedere un adversar PPT?

1. $f(n) = 2$
2. $f(n) = 1/2000$

3. $f(n) = 1/n^{2000}$
4. $f(n) = 1/2^{n/2}$
5. $f(n) = f1(n) + f2(n)$, unde $f1(n)$ și $f2(n)$ sunt neglijabile
6. $f(n) = f1(n) + f2(n)$, unde $f1(n)$ este neglijabilă și $f2(n)$ este ne-neglijabilă

4)

1. neneglijabil

2. neneglijabil

3. neneglijabil

4. neglibajil

5. neglijabil

6. neneglijabil

I. Atribuiți fiecărui termen definiția corespunzătoare. Definițiile au fost preluate din glosarul de termeni *NIST – Computer Security Resource Center* [1]. Puteți citi mai multe despre *phishing* în documentul *European Union Agency for Cybersecurity* (ENISA) dedicat acestui subiect [2].

(A) - 4

(B) - 2 (A) Inginerie socială

(c) - 1 (B) Phishing

(D) - 3 (C) Whaling

(E) - 6 (D) Pharming

(F) - 5 (E) Spear phishing

LAB 5 (F) Spoofing

(1) Un tip specific de phishing care vizează membrii de rang înalt ai organizațiilor.

(2) O tehnică pentru încercarea de a achiziționa date sensibile, cum ar fi numerele de cont bancar, printr-o solicitare frauduloasă prin e-mail sau pe un site web, în care făptuitorul se maschează ca o afacere legitimă sau o persoană de încredere.

(3) Utilizarea mijloacelor tehnice pentru a redirecționa utilizatorii către accesarea unui site Web fals, mascat drept unul legitim și divulgarea informațiilor personale.

(4) O încercare de a păcăli pe cineva să dezvăluie informații (de exemplu, o parolă) care pot fi folosite pentru a ataca sisteme sau rețele.

(5) Falsificarea adresei de trimitere a unei transmisii pentru a obține intrarea ilegală într-un sistem securizat.

(6) Un termen colocvial care poate fi folosit pentru a descrie orice atac de phishing foarte vizat.

RNG - random number generator

de trei tipuri - true, pseudo, hybrid

true rng => generatoare care sunt direct implementate in calculatoare, ele se bazeaza pe procese fizice (temperatura, viteza procesor) folosind aceste procese, trng genereaza numere

pseudo rng => sunt procese deeterministe care are un program care e determinat dinainte, si parametru seed (mereu incepe de la un seed)

hybrid rng => combinatie intre cele 2. Are proprietatea ca ne da in biti aleatori, dar viteza e destul de joasa pt ca trb sa isi capteze fiecare seed, dar fiind si un prng o sa fie proces rapid. Prin cele doua combinate iti generezi destuli biti ai sa iti umplii seed ul

folosind un trng care este mereu incet, generam o secventa de nr sau biti (in general) si aceasta secventa o folosim pe post de seed la PRNG (viteza mare)

RNG e o functie f: N -> N sau R sau int [...] sau multime M sau pe {0,1}

Dati k biti aleatori consecutivi, un atacator nu trebuie sa fie capabil sa determine al k+1 lea bit(sau cel cu nr 0) cu o probabilitate mai mare decat 1/2;

Lab8

I.

a)A

b)F

c)A

d)A

e)F

f)F

g)F

Răspundeți cu *adevărat* sau *fals* pentru fiecare dintre următoarele afirmații. Căutați online informații despre funcțiile hash menționate.

a) *Amestecarea ingredientelor pentru realizarea unei prăjituri poate fi considerată one-way function.*
b) *Funcția hash MD5 este considerată sigură la coliziuni.*
c) *SHA256 este o funcție hash cu output pe 256 biți.*
d) *Valoarea hash SHA-1 pentru cuvantul „laborator" este 0x4bcc6eab9c4ecb9d12dcb0595e2aa5fbc27231f3.*
e) *Este corect să afirmăm că „o funcție hash criptează".*
f) *O funcție hash folosită pentru stocarea parolelor trebuie să fie rapidă (i.e., să se calculeze rapid H(x) pentru x dat).*
g) *Hash-ul (fără salt) - 095b2626c9b6bad0eb89019ea6091bd9 – corespunde unei parole sigure, care nu ar fi susceptibilă spre exemplu la un atac de tip dicționar.*

Lab9

RSA

criptosistem cu cheie publica

creat din 3 faze:

- setup -> 2 nr prime p si q >2 * => p x q = n;

generam un nr e ($<-) din Z fi(n)

fi(n) este nr numerelor care sunt mai mici decat n si prime cu n

daca avem un fi de p, p prim cate nr < p exista si prime cu el => f(p) = p-1

p e nr prim

fi(n) = fi(p q) = (p-1)(q-1)

In total avem pq-p-q+1= p(q-1)-(q-1) = (p-1)(q-1)

avem nevoie de un d ai e*d congruent 1(PROD fi(N))

d -cheie decript

e-cheie encript

La finalul setup ului avem parametrii publici: (n,l)

Cheia privata (secreta) sunt nr : p,q,d -> daca sunt obtinute de atacatori e o probl!!!!!!

cmmdc dintre e si fi(n) trb sa fie 1

Encript: o functie care are nevoie de un mesaj m si de cheia e

m face parte din Z de n (mesajul nostru)

pt a obtine cipher textul il ridicam pe m la puterea e

c = m^e(mod n)

decript: (c,d,n)

mesaj m = c^d(mod n)

Corectitudinea: m' = c^d = m(^e)^d = m^ed

Th Lagrange -> oricare ar fi x apart G grup, x^|G| = 1(G) adica ordinul grupului

m ap Z(n)

ord(Z(n)) = fi(n) = (p-1)(q-1)

p,q,d sunt param privati = cheie secreta

daca d este aflat de atacator => toate mesajele criptate vor fi aflate

daca p sau q sunt aflate => atacatorul poate afla q sau p si poate calcula fi(n) = (p-1)(q-1)

stiind n si e (cheie publica) => poate calcula d folosind alg Euler pt cmmdc

problema factorizarii =>

Date p si q doua nr prime, si n = p*q, este dificil de a gasi divizorii p si q pornind doar de la n

e = 65537 = 2^2^4 +1

Se consideră cheia publică RSA cu modulul pe 128 biți:

```
N=234841136411758273000763594354834942653
e=65537
```

Factorizați modulul, i.e. determinați valorile p și q [1]. Calculați apoi coeficientul de decriptare d [2].

Ex. I

N=234841136411758273000763594354834942653

e=65537

Factorizați modulul, i.e. determinați valorile p și q[1]. Calculați apoi coeficientul de decriptare d[2].

1 | 14086963408384851001 | 16670813262138239653 | 234841136411758273000763594354834942653 (4 divisors)

p = 14086963408384851001

q = 16670813262138239653

fi(n) = (p-1)(q-1) = 14086963408384851000 * 16670813262138239652 =

= 234841136411758272970005817684311852000

d = e^(-1) mod fi(n)

e·d≡1(mod ϕ(N)) => d = 131139372709478882400526464589358085473

The public key is (n, e) and the private key is (n, d)

Lab10

1. ***Securizarea codului***

Marcați cu *Adevărat* (A) sau *Fals* (F) afirmațiile de mai jos.

a) A
b) F
c) A
d) A
e) A
f) F
g) A
h) F

a) Ca să analizați/testați securitatea aplicației, ajută să gândiți ca un atacator.
b) Pentru că sunt foarte multe, din punct de vedere al logicii/design-ului aplicației, nu încercați să acoperiți toate cazurile posibile pentru a preveni un comportament neașteptat.
c) Întotdeauna validați câmpurile de input, atât ca format (tip de date, protejare împotriva SQL injection, etc.) dar și ca valori (dimensiuni, valori minime/maxime, verificări între diferite câmpuri de input; ex. data de început a unei activități anterioară datei de final, prețurile să aibă valori pozitive, etc.)
d) Aveți în vedere vulnerabilități de tip buffer overflow.
e) În general nu e o practică bună să stocați log-uri, pentru că ocupă spațiu și cresc timpul de așteptare al utilizatorului.
f) Oferiți cât mai multe detalii posibile utilizatorilor când eșuează autentificarea prin username și parolă sau când implementați mecanisme de recuperare a parolei, pentru a facilita accesul acestora (spre exemplu menționați „Adresa de e-mail nu corespunde unui cont activ" la încercarea de a recupera parola prin e-mail).
g) Nu rețineți parole în clar.
h) Hardcodați parole în cod.