C

1. Adja meg a következő fogalmakat!
   a. ransomware (zsarolóprogram)
   b. hitelesség
   c. üzenet visszajátszás

Ransomware
- Fájltitkosító ransomware
- Nem titkosító ransomware
- Böngészőlezáró ransomware

Olyan kártékony program meg lezárja a felhasználó fájljait, blokkolja az áldozat hozzáférését a számítógéphez és az okozott károk visszafordításáért minden esetben váltságdíjat követel.

Képesek lehetnek az áldozat érzékeny személyes adatainak megszerzésére, védelmi szoftverek leállítására, megtévesztő figyelmeztetések megjelenítésére és más kéretlen tevékenységekre is.

Gyakran drive-by-download útján terjednek.

Hitelesség
- Felhasználó hitelesítése
- Üzenet hitelesítő kód

Valaminek a forrása az amit megjelöltek, és a tartalma az eredeti.

Felhasználó hitelesítése:

Az a folyamat, amikor egy entitás meggyőződik egy másik entitás identitásáról.

Üzenet hitelesítő kód:

Egy rövid, fix hosszúságú érték, mely lehetővé teszi az üzenet sértetlenségének és forrásának ellenőrzését, de nem biztosítja a letagadhatatlanságot.

- Üzenet visszajátszása: (passzív támadás)

A támadó lehallgatja az üzenetet, majd újra elküldi.

Az adatátvitel lehalgatása, monitorozása. Ilyen támadás esetén továbbított adat megszerzése a célunk.
Nehéz észrevenni, hiszen az átküldött adat nem módosul.

2. Mi a CIA hármas? Példákkal magyarázza meg a fogalmakat!

BSR

CIA – Biztonsági célok

Confidentiality / Bizalmasság

Titkos / személyes információk nem kerülhetnek jogosulatlanok kezébe. Adatok tárolásánál feldolgozásánál, továbbításánál biztosítani kell

Integrity / Sértetlenség

Adatintegritás: Adat nem módosul tárolása, feldolgozása, továbbítása során

Rendszerintegritás: Rendszer az elvártak szerint működik, jogosulatlan módosításoktól mentes

Availability / Rendelkezésre állás

A szolgáltatás a jogosultak számára szükséges időben, szükséges ideig használható

2. Mi a CIA háromszög?
3. Jellemezze a vírusokat! Csoportosítsa a vírusokat célpontjuk és rejtőzködésük alapján! Ismertesse az egyes csoportok jellemzőit!

Vírusok

Végrehajtható programokat, vagy dokumentumokat fertőzi meg
Gyakoriak script kódok – MS Office, Adobe PDF
Vírus a kód lefuttatásával valami kárt okoz

Megfertőzhet:

- Alkalmazásokat
- Rendszerfájlokat
- Bootnál futtatott programkódot

Részei:

Fertőző mechanizmus: Hogyan terjed, sokszorozódik a vírus
Indíték: Esemény, feltétel mely meghatározza mikor aktiválódik a büntető rutin – Logikai bomba
Büntető rutin: Kárt okozó tevékenység

Célpont szerinti csoportosítás

Boot vírusok
Háttértár boot szektorába ágyazódik be
OS előtt aktiválódik, összes többi háttértárat megfertőzi

Alkalmazásvírusok
Append és replace vírusok, letöltödnek a memóriába, megfertőzik a többi futó programot

Macrovírus
Makrókat támogató dokumentumszerkesztőket támadnak meg, terjedéshez elég csak megnyitni egy fertőzött állományt
Ide tartoznak a levelező vírusok

Rejtőzködési stratégia szerinti csoportosítás

Titkosított vírus
Titkosítja a tartalmát

Lopakodó vírus
Memóriában maradva cselezi ki az OS-t és antivírust, innen változtathat OS jellemzőin, könyvtárstruktúrán
Rootkitek: Eszköz, melyet root (legnagyobb jogosultság) megszerzése után használ

Polimorf vírus
Fertőzési ciklusonként változtatják megjelenési formájukat – nehéz felismerni
Mutációs motor felel a kulcsgenerálásért, titkosításért ez is módosul

Metamorfózisra képes vírus
Minden alkalommal teljesen felülírják magukat / kinézetüket

4. Mi a gyökércsomag és a hátsóajtó? Milyen védekezési módot ismer?

Gyökércsomag (Rootkit)

- Perzisztens
- Memória alapú
- Felhasználó módú
- Kernel módú

A gyökércsomag egy programcsomag, mely installálása után fedett hozzáférést biztosít és tart fent a már fertőzött géphez adminisztrátori jogosultságokkal. Az operációs rendszer valamennyi funkciójához és szolgáltatásához hozzáférést ad.

A gyökércsomagok hátsóajtó hozzáférést is biztosítanak trójaiak számára.

Adminisztrátori jogosultsággal a támadónak teljes kontrollja van a rendszer felett. Felrakhat és módosíthat programokat, fájlokat, processzeket monitorozhat, hálózati forgalmat fogadhat és küldhet. A gyökércsomag ezeket a mechanizmusokat elrejti.

Perzisztencia alapján megkülönböztetünk perzisztens és memória alapú gyökércsomagot:

- Perzisztens gyökércsomag:

  A gyökércsomag perzisztens helyen tárol kódot, pl. registry-ben.

- Memória alapú gyökércsomag:

  Mivel csak a memóriában van benne, így nincs perzisztens kód, tehát az újraindítást nem éli túl, viszont nehezebb detektálni.

Létezik "felhasználó módú" és "kernel módú" gyökércsomag:

- Felhasználó módú:

  Felhasználói szinten működik az operációs rendszerben. Lehallgatja az API hívásokat és módosítja az azokra kapott választ, hogy elrejtse magát.

- Kernel módú:

  A gyökércsomag úgy rejti el jelenlétét, hogy módosítja a kernelt.

  A kernel az operációs rendszer alapja, amely felelős a hardver erőforrásainak kezeléséért.

  A korai rootkitek felhasználói módúak voltak. Az általuk alkalmazott változtatásokat kernel kódokkal lehetett detektálni.

  Az új generációs rootkitek kernel szintű változtatásokat hajtanak végre és a rejtőzködéshez az elsődleges célpontjaik a rendszerhívások.

Hátsóajtó (Backdoor)

A program egy titkos belépési pontja, mely lehetővé teszi, hogy a belépési pont ismerője a biztonságos hitelesítés nélkül kapjon hozzáférést.

Programozok legálisan is használtak már hátsaajtókat programok tesztelésére. A hátsóajtó akkor válik veszélyessé, amikor azt tisztességtelen programozók használják illetéktelen hozzáférésre.

A védelmi intézkedések ez ellen szoftverfejlesztésekre és szoftver updatekre irányulnak.

4. Mi a gyökeresítés

5. Ismertesse az RSA-FDH digitális aláírás algoritmusait!

A

1. Adja meg a következő fogalmakat!
   a. CIA hármas
   b. sérülékenység
   c. kártékony program
   d. nulladik napi támadás

Sérülékenység / vulnerability

Informatikai rendszer gyengesége, amelyen keresztül valamely fenyegetés megvalósulhat

Kategóriák:

- Rendszerelem, adatok módosulása
- Rendszerelem, adat kiszivárgása
- Rendszerelem elérhetősége lassú, vagy elérhetetlen / használhatatlan

c. kártékony program

Adatok / szoftverek bizalmasságát, integritását, rendelkezésre állását veszélyezteti, vagy erkölcsi / anyagi / idő kárt okoz

d, nulladik napi támadás: Valamely számítógépes alkalmazás olyan sebezhetőséget használja ki, ami még nem került publikálásra, a szoftver fejlesztője nem tud róla, vagy nem érhet® még el azt foltozó biztonsági javítás.

2. Ismertesse a hálózati kommunikáció aktív támadásait!

Aktív támadások:

Adatfolyam módosítása, hamis üzenet generálása.
Nehéz teljesen megelőzni
Példák:
- Megszemélyesítés adatmódosítás
- Üzenet visszajátszás
- DDOS

- Megszemélyesítés:

A támadó eljátsza a legális fél szerepét. Általában ehhez a támadáshoz szükséges valamely másik aktív támadás.

- Üzenet visszajátszása:

A támadó lehallgatja az üzenetet, majd újra elküldi.

- Adat módosítása:

A támadó az üzenetek valamely részét, vagy sorrendjét megváltoztatja

- Terheléses támadás (DDOS):

A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat.

3. Mi a Fejlett Perzisztens Fenyegetés (APT)? Milyen technikákat alkalmaz? Ismertessen egy példát!

Fejlett Perzisztens Fenyegetés = Advanced Persistent Threat (APT)
- Fejlett
- Perzisztens
- Fenyegetés

Kiberbűnözés, mely üzleti és politikai célpontokat célozzák meg, többféle behatoló technológia és kártékony program alkalmazásával.

APT-k különböznek a többi támadástól a célpont körültekintő kiválasztása miatt. Információt gyűjt, hogy pl. megállapítsa az alkalmazott szerepét és hozzáférési szintjét. Amennyiben ez nem vezet célra, akkor más felhasználók után kutathat, akik jobb pozícióban, több privilégiummal rendelkeznek. Nem egyszerűen feltöri a szervezet infrastruktúráját, sokkal inkább az alkalmazottakra koncentrálnak.

A speciális célpont és a perzisztens jellegük miatt a védekezés nem kivitelezhető hatékonyan csupán hagyományos biztonsági eszközök bevetésével. Többféle technikai védintézkedés kombinációjának alkalmazása és oktatás ajánlott.

- Fejlett:

A támadók számos eszközt használnak fel céljuk eléréséhez. Céljuk, hogy elkerüljék a célkeresztbe állított rendszert körülölelő vagy az abban működő védelmi eszközöket. A támadók alkalmazkodnak a védők erőfeszítéseihez.

- Perzisztens:

A támadók egy jól meghatározott céllal tevékenykednek, és többnyire nem véletlenszerűen, találgatás útján próbálnak rájönni, hogy milyen sebezhetőségeket tudnak kihasználni, hanem már felkészülten, alapos felderítőmunka után lépnek akcióba. Ameddig nem érik el céljukat, addig nem hagyják el a rendszert. Gondoskodnak arról, hogy a hozzáférésük fenntartható legyen.

- Fenyegetés:

Ez esetben célzott, irányított és komplex akciókról beszélünk, amelyek komoly fenyegetést jelenthetnek az informatikai rendszerekre és az adatokra.

4. Jellemezze a férgeket! Ismertesse a terjedési módjait! Ismertesse rejtőzködési módjait! Adjon meg két kliens oldali sebezhetőséget!

Kliens és szerver oldali szoftver sebezhetőségek kiaknázásával férnek hozzá számítógépekhez.
Önsokszorosítóak, nincs szükségük gazdaprogramra.

Terjedési technikák:

- Hálózati kapcsolatokon keresztül rendszerről rendszerre terjedhetnek
- Megosztott médiákon, USB driveon, CD-n, DVD-n keresztül
- E-mail vagy üzenőfal segítségével

Terjedés során általában a következőket hajtja végre:

- Megfelelő hozzáféréseket keres host táblákban, címtárakban vagy cserélhető médiákat keres
- Ezekkel a hozzáférési mechanizmusokkal lemásolják magukat távoli rendszerekre és végrehajtódnak

5. Mi a zsarolóprogram? Ismertesse a fajtáit!

- Fájltitkosító ransomware
- Nem titkosító ransomware
- Böngészőlezáró ransomware

Olyan kártékony program meg lezárja a felhasználó fájljait, blokkolja az áldozat hozzáférését a számítógéphez és az

okozott károk visszafordításáért minden esetben váltságdíjat követel.

Képesek lehetnek az áldozat érzékeny személyes adatainak megszerzésére, védelmi szoftverek leállítására, megtévesztő

figyelmeztetések megjelenítésére és más kéretlen tevékenységekre is.

Gyakran drive-by-download útján terjednek.

6. Definiálja a hash függvényt! Ismertesse a kriptográfiai hash függvény biztonsági elvárásait!

def: A H : $\{0, 1\}^* \rightarrow \{0, 1\}^n$, n ∈ N függvényt hash függvénynek nevezzük.
elvárások:
Őskép ellenálló: Adott y ∈ Y értékhez, nehéz olyan x ∈ X értéket megadni, hogy H(x) = y. Második őskép ellenálló(gyengén ütközésmentes): Adott x értékhez nehéz olyan x 0 értéket találni, hogy x 6= x 0 és H(x) = H(x 0).
Ütközésmentes(erősen ütközésmentes): Nehéz olyan x, x 0 ∈ X értékeket találni, hogy H(x) = H(x 0).

Jellemzői, elvárásai:

Őskép ellenálló: y-hoz nehéz olyan x, hogy $H(y) = y$
Második ősképellenálló: x értékben nehéz olyan x' -t találni, hogy $x \neq x'$ és $H(x) = H(x')$
Ütközésmentes: Nehéz olyan $x, x' \in X$ értéket találni, hogy $H(x) = H(x')$

Ismertesse az RSA-FDH digitális aláírási sémát!

RSA FDH – Full Domain Hash

Megoldja az első problemákat – Az üzenetet hasheljük mielőtt aláírjuk

`DS = (Key, Sign, Ver)`

Key:

- Véletlenül választunk két nagy prímet: $p \cdot q$
- Kiszámítjuk az RSA modulus: $n = p \cdot q$
- Kiszámítjuk n Euler-féle $\emptyset$ függvény értékét: $\emptyset(n) = (p-1)(q-1)$
- Véletlenül választunk egy e egészet, ahol $1 < e < \emptyset(n)$ és $(e, \emptyset(n)) = 1$
- Kiszámítjuk: d: $1 < d < \emptyset(n)$, ahol $ed \equiv 1 \ (mod \ \emptyset(n))$

$PK = (n, e), SK = d$ és $\emptyset(n), p, q$ titkos paraméterek

$M = \{0,1\}^*, S = Z_n$

Sign:

- $Sign_{SK}(m) = H(m)^d (mod\ n)\ \forall m \in M$, ahol $SK = d, H: \{0,1\}^* \rightarrow Z_n$ hash függvény.

Ver:

- $Ver_{PK}(m,s) = \begin{cases} TRUE, & S^e \equiv H(m)\ mod(n); \\ FALSE, & egyébként \end{cases}$

$\forall (m,s) \in M \times S$, ahol $PK = (n, e)$

B

1. Adja meg a következő fogalmakat!
   a. informatikai biztonság fogalma
   b. hitelesség
   c. kockázat

Informatikai biztonság egy rendszer olyan állapota, melyben a kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása biztosított, valamint a rendszerelemek sértetlensége és rendelkezésre állása szempontjából zárt, teljese körű, folytonos és kockázatokkal arányos.

b, hitelesség: Valaminek a forrása az, amit megjelöltek, és a tartalma az eredeti.

- Felhasználó hitelesítése (Entity Authentication): Az a folyamat, amikor egy entitás meggyőződik egy másik entitás identitásáról.
- Üzenet hitelesítő kód (Message Authentication Code): Egy rövid, fix hosszúságú érték, mely lehetővé teszi az üzenet sértetlenségének és forrásának ellenőrzését, de nem biztosítja a letagadhatatlanságot.

Kockázat / risk
Fenyegetettség mértéke, amely valamely fenyegető tényezőből ered
A kockázat fenyegetés bekövetkezésének gyakorisága és az az által okozott kár nagyságának függvénye
Cél a minimalizálása

2. Ismertesse a biztonsági tervezési alapelveket!

Tervezési alapok

Jogosultságok minimalizálása
Csak annyi jogosultságot adjunk, amennyi feltétlen szükséges
Preventív intézkedés csökkenti a véletlen / direkt károkozást
Bármely rendszernél alkalmazható

Minimalizálás
Rendszerkonfiguráció minimalizálása
Olyan szoftvert, alkalmazást ne futtassunk, melyek nem feltétlen szükségesek a biztonságos működéshez
Növeli a teljesítményt, tárhelyet takarít meg
Ha csak emailezik egy gép, ne legyen rajta más

Több szintű védelem
Több szintű, többféle védelem – Preventív, detektív, korrektív

Open Design
Biztonsági mechanizmus elemei, működés módja nyilvános kell legyen
Szakértők elemezik az algoritmusokat – bizalom
Kirchhoff-elv

Felosztás / compartmentalization
Parcellák / terek kialakítása, elkülönítése
Limitálja a kárt, ha az egyik sérül, a többi még rendben van

Egyszerű megoldást válasszunk
Összetett rendszer – nem jó
Egyszerű rendszert könnyebb tervezni, implementálni, tesztelni

Pszichológiai elfogadottság
Ha egy mehcanizmus gátolja valami könnyű / kényelmes hozzáférését, használatát, a felhasználó ki fogja kapcsolni
Biztonsági mechanizmus legyen transzparens, kövesse az emberi gondolkodást

2. Ismertesse a biztonsági tervezési alapelveket!
3. Ismertesse a környezeti fenyegetéseket és az ellenük való védekezést!

Fenyegetések

Hardver
Rendelkezésre állásra irányul a legtöbb fenyegetés
Véletlen, vagy szándékos rongálás / lopás – sérülhet vele a bizalmasság
Védelem: Fizikai és adminisztratív intézkedések

Szoftver
Rendelkezésre állásra irányuló fenyegetés – alkalmazás törlése, módosítása
Védelem: backup
Sértetlenségre irányuló fenyegetés – szoftver módosítása, vírusok
Szoftverkalózkodás

Adat
Védeni kell, értékes és egyedi
Továbbítás, tárolás, feldolgozás során sérülhet
Bizalmasságra irányuló fenyegetés – Személyes adatok, tervek, stb
Sértetlenségre irányuló fenyegetés – adatok módosítása
Rendelkezésre állásra irányuló fenyegetés – Adat törlése

5. Mia zombi és a botnet? Mire használhatóak?

Zombi számítógép: Internethet kapcsolódó gép, melyet a támadó irányít, erőforrásokat felhasználja

Támadó ügynökök

Kártékony kód a támadó irányítása alá helyezi a rendszert, annak erőforrásait – Zombi gépek
Zombi gépek hálózatra kötve botnet
Rendszer integritása, rendelkezésre állása veszélyben

Zombik használata

- DDOS
- Spam
- Forgalomfigyelés
- Keylogging
- Malware terjedés
- Adware

botnet: olyan hálózatra kapcsolt gépek összessége, amelyek felett átvették az irányítást.
használata: botneten keresztül zombi gépek használata

7. Ismertesse a titkosítási sémákkal szembeni támadásokat!

Támadások

Támadó célja

- Titkos visszafejtő kulcs megszerzése
- Egy adott titkosított üzenethez tartozó nyílt üzenet megszerzése

Támadási módok

Csak a titkosított üzenet ismert – LOA

A támadó rendelkezésére áll ugyanazon kulccsal titkosított üzenetekből álló lista

Ismert nyílt üzenet alapú támadás – KPA

A támadó rendelkezésésre áll egy ugyanazon kulccsal titkosított nyílt és titkosított üzenetekből álló lista.
Cél a titkos kulcs, vagy a listán nem szereplő titkosított üzenethez tartozó nyílt üzenet megszerzése.

Választott nyílt üzenet alapú – CPA

A támadó rendelkezésére áll egy ugyanazon kulccsal titkosított nyílt és titkosított üzenetből álló lista, ahol a nyílt üzenetek a támadó által választottak
Nem alkalmazkodó → passzív, a támadó előre kiválasztja a nyílt üzeneteket
Alkalmazandó → aktív, a kapott titkosított üzenetek alapján választja ki a következő nyílt üzenetet
Cél a titkos kulcs, vagy a listán nem szereplő kulcsot üzenethez tartozó nyílt üzenet megszerzése

Választott titkosított üzenet alapú – CCA

A támadó rendelkezésére áll egy ugyanazon kulccsal titkosított nyílt és titkosított üzenetekből álló lista, ahol a titkosított üzenetek a támadó által választottak.
Cél ugyanaz mint előbb

3. Ismertesse a Nyilvános Kulcs Infrastruktúra (PKI) elemeit I

Regisztrációs hivatal – RA

(Polgár Jenő hivatal)
(meg akarok halni)

Feladata:

- Ügyfelek megbízható hitelesítése
- Tanusítványkérés összeállítása, továbbítása
- Tanusítvány visszavonási kérések fogadása

Hitelesítő hivatal – Certification Authority

Feladata:

- Tanúsítványkérések fogadása
- Kulcspárok generálása a különböző implementációkban
- Nyilvános kulcsú tanusítványok kialakítása
- Kiadott tanusítványok közzététele nyilvános tanusítványtárban
- Korábbi tanusítványok / kulcspárok megújítása
- Tanusítványok visszavonása, ezek listájának publikálása

Tanusítványtár

Speciális adatbázis, amely tartalmazza

- CA által kibocsátott tanusítványokat
- Visszavont tanusítványok listáját
- Egyéb adatokat a tanusítványoknál

Feladata:

Bármely tanusítvány állapotáról real-time információ adása

Szolgáltatásai:

Biztosítja ügyfeleket egy adott tanusítvány hitelességéről, érvényességéről

6. Ismertesse a permutációs titkosítási sémát!

A nyílt üzenetet n hosszúságú blokkokra osztjuk. A kulcs egy permutáció. A titkosítás során a kulcs alapján permutáljuk a betűknek megfelelő Zv -beli értéket.

P = C = Z n v , ahol v az abc és n a blokk mérete

K = {(1, . . . , n) összes lehetséges permutációja}

Key: $\pi \in K$ véletlenül választott

Enc: $\forall m = (m1, m2, \ldots, mn) \in Z^n_v$ esetén

$Enc_\pi(m1, m2, \ldots, mn) = (m\pi(1), m\pi(2), \ldots, m\pi(n))$

Dec: $\forall c = (c1, c2, \ldots, cn) \in Z^n_v$ esetén

$Dec_\pi(c1, c2, \ldots, cn) = (c\pi{-}1(1), c\pi{-}1(2), \ldots, c\pi{-}1(n))$

7. Adja meg a digitális aláírás fogalmát!

7. Adja meg a digitális aláírás fogalmát!

A digitális aláírási séma egy DS = (Key, Sign, Ver) hármas, ahol

- Key: A Key kulcsgeneráló algoritmus a k biztonsági paraméterre kiszámítja a (PK, SK) kulcspárt, ahol PK nyilvános és SK titkos.
- Sign: A Sign aláíró algoritmus az SK titkos kulcshoz és az $m \in \{0, 1\}*$ üzenetre generál egy s = SignSK (m) aláírást.
- Ver: A Ver ellenőrző® algoritmus a PK nyilvános kulcsra, az m üzenetre, és az s aláírásra IGAZ vagy HAMIS értéket ad vissza. IGAZ esetén az aláírás érvényes, HAMIS esetén érvénytelen

DS = (Key, Sign, Ver) digitalis aláírási séma, ahol

Key: Kulcsgeneráló algoritmus k parameter alapján kiszámítja a (PK, SK) kulcspárt

Sign: Aláíró algoritmus, m üzenetre SK titkos kulccsal generál aláírást

$$S = Sign_{SK}(m)$$

Ver: Ellenörző algoritmus, mely S aláírásra és PK nyilvános kulcsra True vagy False értéket ad, attól függően, hogy az aláírás érvényes-e

8. Ismertesse az RSA titkosítási sémát!

8. Ismertesse az RSA titkosítási sémát.

1. Véletlenül választunk két nagy prímet: p, q.
2. Kiszámítjuk az RSA modulust: n = p · q.
3. Kiszámítjuk n Euler-féle ϕ függvény értékét: ϕ(n) = (p − 1)(q − 1).
4. Véletlenül választunk egy e egészt, ahol 1 < e < ϕ(n) és (e, ϕ(n)) = 1.
5. Kiszámítjuk: d: 1 < d < ϕ(n), ahol ed ≡ 1 (mod ϕ(n)).

PK = (n, e), SK = d és ϕ(n), p, q titkos paraméterek

M = S = Zn

SignSK (m) = md (mod n) ∀m ∈ M, ahol SK = d.

VerPK (m,s) = TRUE, s e ≡ m (mod n); FALSE, egyébként.

∀(m,s) ∈ M × S, ahol PK = (n, e).

RSA séma

AE = (Key, Enc, Dec) asszimetrikus séma

Key:

1. Két nagy prím: p, q
2. Kiszámítjuk az RSA modulust: $p = P \cdot q$
3. Kiszámítjuk az Euler féle ϕ függvényt: $\theta(n) = (P-1) \cdot (q-1)$
4. Választunk egy véletlen e egészet: $1 < e < \theta(n)$ *és* $(e, \theta(n)) = 1$
5. Kiszámítjuk d-t: $1 < d < \theta(n)$ *és* $ed = 1 (mod\ \theta(n))$

e a titkosító $PK(n, e)$ $P = C = Z$

d a visszafejtő $SK(n, d)$

$Enc_{PK}(m)$: $m^e (mod\ n)$ *és* $PK = (n, e)$

$Dec_{sK}(c)$: $c^d (mod\ n)$ *és* $SK = (n, d)$

6. Ismertesse az eltolásos titkosítási sémát.

$P = C = K = Z_v$, ahol v az abc mérete

Key: $K \in Z_v$ véletlenül választott

Enc: $\forall m \in Z_v$ esetén $Enc_K(m) = m + K \pmod{v}$

Dec: $\forall c \in Z_v$ esetén $Dec_K(c) = c - K \pmod{v}$