Matematikai fogalmak

Minta

5.1.1. A minta és a minta realizáció A matematikai statisztika szemléletmódja szerint a megfigyelendő mennyiség valószínűségi változó. Jelöljük ezt a valószínűségi változót X-szel. Figyeljük meg X-et n-szer, egymástól függetlenül. Jelölje $X_1, X_2, \ldots, X_n$ a megfigyelési eredményeket. Ezeket a megfigyelési eredményeket nevezzük mintának. Azonban $X_1, \ldots, X_n$-et sem egy szám n-esnek tekintjük, hanem olyan objektumnak, amely magába sűríti a megfigyelések eredményeként adódó összes lehetséges szám n-est. Így az $X_1, \ldots, X_n$ mennyiségeket is valószínűségi változóknak tekintjük.

Az $X_1, X_2, \ldots, X_n$ független, azonos eloszlású valószínűségi változókat *mintának* nevezzük. Rögzített $\omega \in \Omega$ esetén az $x_1 = X_1(\omega), x_2 = X_2(\omega), \ldots, x_n = X_n(\omega)$ szám n-est *minta realizációnak* nevezzük. (Itt Ω a háttérben lévő eseményteret jelöli.)

5.1.1. NOTE. 1. A gyakorlatban mindig minta realizációkat figyelünk meg. Ezek azonban megfigyeléssorozatonként különböznek egymástól. A minta elméleti fogalma az összes lehetséges realizációt magába foglalja.

2. Ha X egy valószínűségi változó, akkor X-re vett minta alatt az X-szel azonos eloszlású, független $X_1, X_2, \ldots, X_n$ valószínűségi változókat értjük.

3. Ha F egy eloszlásfüggvény, akkor F eloszlásfüggvényű populációból vett minta alatt független, F eloszlásfüggvényű $X_1, X_2, \ldots, X_n$ valószínűségi változókat értünk.

4. A statisztika bizonyos fejezeteiben a fentinél tágabban értelmezik a minta fogalmát. Például a többdimenziós statisztikai analízisben az $X_1, \ldots, X_n$ valószínűségi változók többdimenziósak, míg az idősorok analízisében a függetlenség (illetve az azonos eloszlás) feltétele nem teljesül.

Becslések

6.1.1. DEFINITION. A T statisztikát a t paraméter *torzítatlan becslésének* nevezzük, ha $\mathbb{E}T = t$.

A torzítatlanság azt jelenti, hogy a becslés a becsülendő paraméter körül ingadozik.

6.1.2. DEFINITION. A T_n sorozatot a t paraméter *konzisztens* (*erősen konzisztens*) *becslésének* nevezzük, ha $T_n \to t$ sztochasztikusan (majdnem biztosan).

6.1.1. A maximum-likelihood-becslés A *maximum-likelihood elv* szerint az ismeretlen paraméter azon értékét fogadjuk el, amely mellett a bekövetkezett eredmény maximális valószínűségű.

6.1.4. DEFINITION. Legyen $X_1, \ldots, X_n$ minta egy diszkrét eloszlásból, $x_1, \ldots, x_n$ pedig a minta realizáció. Legyen ϑ az ismeretlen paraméter. Az

$$L(x_1, \ldots, x_n; \vartheta) = P(X_1 = x_1, \ldots, X_n = x_n) = \prod_{i=1}^{n} P(X_i = x_i)$$

függvényt *likelihood-függvénynek* nevezzük. Az

$$l(x_1, \ldots, x_n; \vartheta) = \log L(x_1, \ldots, x_n; \vartheta)$$

függvényt pedig *loglikelihood-függvénynek* hívjuk.
A maximum-likelihood elv szerint L-et kellene maximalizálni ϑ szerint. A maximum hely azonban pontosan egybeesik l maximumhelyével, hiszen a természetes alapú logaritmus függvény szigorúan monoton növekvő. Így elegendő az l maximumhelyét meghatározni.

Konfidenciaintervallumok

6.1.2. Konfidencia intervallumok Legyen ϑ ismeretlen paraméter, T_1 és T_2 két statisztika. Azt mondjuk, hogy a $[T_1, T_2]$ intervallum $1 - \alpha$ *megbízhatósági szintű konfidencia intervallum* ϑ-ra, ha

$$P(\vartheta \in [T_1, T_2]) \geq 1 - \alpha.$$

Itt α szokásos értékei 0.1, 0.05, 0.01.

Átlag

Számtani vagy aritmetikai középértéken n darab szám átlagát, azaz a számok összegének n-ed részét értjük. A számtani közepet általában A betűvel jelöljük:

$$A(a_1; \ldots; a_n) = \frac{a_1 + \ldots + a_n}{n}.$$

U-próba

6.2.1. u-próba. A statisztikai hipotézisek vizsgálatára próbákat (teszteket) alkalmazunk. A legegyszerűbb próba az u-próba.

Legyen $X_1, \ldots, X_n$ minta $\mathcal{N}(0,1)$ eloszlásból. Tegyük fel, hogy σ^2 ismert. Az m várható értékre az előírás m_0. Tehát a

$$H_0 : m = m_0$$

nullhipotézist kell vizsgálnunk a

$$H_1 : m \neq m_0$$

altenatív hipotézissel (ellenhipotézissel) szemben. H_0 fennállása esetén az

$$u = \frac{\overline{X} - m_0}{\sigma}\sqrt{n}$$

statisztika standard normális eloszlású. Tehát ha H_0 igaz, akkor u nagy valószínűséggel belecsik egy $[-u_{\alpha/2}, u_{\alpha/2}]$ intervallumba. Ha ez nem áll, akkor az H_1 teljesülésére utal.

Tehát a döntési eljárás a következő. Adott α értékhez meghatározzuk azt az $u_{\alpha/2}$ értéket, melyre

$$P(-u_{\alpha/2} \leq \mathcal{N}(0,1) \leq u_{\alpha/2}) = \alpha.$$

α az elsőfajú hiba nagysága. Ha $u \notin [-u_{\alpha/2}, u_{\alpha/2}]$, akkor H_0-at $1-\alpha$ szinten (azaz $(1-\alpha)\cdot 100\%$ szignifikancia szinten) elvetjük. Az α értékét 0.1, 0.05, 0.01-nek szoktuk választani.

6.2.3. Kétmintás u-próba Ezzel az eljárással két független, ismert szórású, normális eloszlású valószínűségi változó várható értékének azonosságáról dönthetünk.

Legyenek X $\mathcal{N}(m_1, \sigma_1^2)$, ill. Y $\mathcal{N}(m_2, \sigma_2^2)$ eloszlású független valószínűségi változók, σ_1 és σ_2 ismert paraméterek. X-re vonatkozóan tekintsünk egy n_1, Y-ra vonatkozóan egy n_2 elemű, egymástól független mintát: $X_1, X_2, \ldots, X_{n_1}$; $Y_1, Y_2, \ldots, Y_{n_2}$. Legyen a próba szintje $1-\alpha$. Hipotézisünk:

$$\begin{aligned} H_0 &: m_1 = m_2 \\ H_1 &: m_1 \neq m_2. \end{aligned}$$

A próbastatisztika

$$u = \frac{\overline{X} - \overline{Y}}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}}$$

standard normális eloszlású, ha H_0 fennáll. A továbbiakban hasonlóan járunk el, mint az egymintás u-próba esetén.

Ha $H_1 : m_1 > m_2$ (vagy $m_1 < m_2$) alakú, akkor az egyoldali próbát kell alkalmazni.

6.2.4. Próbák konstrukciója Tegyük fel, hogy 5 mm átmérőjű csapágygolyókat kell gyártani. A minőségellenőrzés során mely tételeket nyilvánítsanak jónak, és melyeket selejtnek? Tegyük fel az egyszerűség kedvéért, hogy a gyártás során csupán az a hiba léphet fel, hogy a berendezés rossz beállítás miatt túl nagy, vagy túl kicsi golyókat gyárt. Vegyünk mintát, azaz mérjük meg n db kiválasztott golyó átmérőjét. Az átmérők átlaga $\overline{x}$. Ha $\overline{x}$ 5 mm közelében van, akkor jók a golyók, ha $\overline{x}$ túl nagy, vagy túl kicsi, akkor selejtesek. De mik legyenek azok a k_1, k_2 kritikus értékek, amelyek alatt, ill. fölött már selejtesnek minősítjük a golyókat? Ehhez segít hozzá az u statisztika:

$$u = \frac{\overline{X} - 5}{\sigma}\sqrt{n}$$

eloszlása $H_0 : m = 5$ esetén standard normális. A standard normális eloszlású valószínűségi változó azonban nagy valószínűséggel egy (u_1, u_2) intervallumban veszi fel értékeit. Ha ezen az (u_1, u_2) intervallumon kívül esik u értéke, akkor arra gondolhatunk, hogy a kiinduló H_0 hipotézisünk nem volt igaz, így H_0-at elvetjük.

A kritikus tartomány megadása azonban nemcsak a H_0 nullhipotézistől, hanem a H_1 alternatív hipotézistől is függ. Tekintsük most azt az esetet, amikor az élelmiszerbolt vezetője a sütödétől 2 kg-os kenyereket vásárol. $H_0 : m = 2$ a nullhipotézis, $H_1 : m < 2$ pedig az ellenhipotézis, amit a boltvezető tekint, hisz számára csak a túl kicsi kenyér a rossz. Így csak akkor fogja a szállítmányt visszautasítani, ha a megmért kenyerek súlyának $\overline{x}$ átlaga túl kicsi. Egyoldali u-próbát alkalmazhat, és a kritikus (elutasítási) tartománya $\overline{x} < k_2$ alakú lesz. Tehát a kritikus tartományt úgy kell megválasztani, hogy a számunkra „rossz" esetektől óvjon.

Mikor jó egy próbastatisztika? Az u-próba esetén ismeretes, hogy ha a valódi m paraméter közel van a nullhipotézisben szereplő m_0 paraméterhez, akkor H_0-at kis eséllyel vetjük el, míg ha távol van tőle, akkor nagy eséllyel vetjük el a H_0-at.

A fentiek alapján a próbastatisztika legyen olyan, hogy

(1) eloszlása pontosan ismert H_0 esetén,

(2) másképpen viselkedjen, ha H_0 nem igaz, mint akkor, amikor H_0 igaz,
(3) ha H_0 „nagyon nem igaz", akkor a próbastatisztika viselkedése térjen el nagyon attól, ahogy H_0 esetén viselkedik.

Ha a fenti elveknek megfelelő próbastatisztikát már megtaláltuk, akkor annak alapján már tudjuk, merre van a jó és merre a rossz. De pontosan hol húzzuk meg a határt a jó (az elfogadási tartomány) és a rossz (a kritikus tartomány) között? Ez az α elsőfajú hiba megválasztásával történik. Ha pl. egy preciziós műszert gyártunk, akkor az alkatrészek közül szigorúan válogatunk: vállaljuk, hogy selejtnek minősítünk egy jó alkatrészt is, semmint véletlenül rosszat építsünk be. Tehát az α elsőfajú hibát nagynak választjuk. Azt azonban, hogy a szokásos α értékek (0.1, 0.05, 0.01) közül melyiket választjuk, a konkrét probléma alapján döntjük el.

Infós fogalmak

Informatikai biztonság fogalma

Az informatikai biztonság az informatikai rendszer olyan, a védő számára kielégítő mértékű állapota, amely az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

- zárt védelem: olyan védelem, amely az összes releváns fenyegetést figyelembe veszi
- teljes körű: a védelmi intézkedések a rendszer összes elemére kiterjednek

- folytonosság: a védelem az időben változó körülmények és viszonyok ellenére is folyamatosan megvalósul
- kockázatokkal arányosság: egy kellően nagy intervallumban a védelem költségei arányosak a potenciális kárértékkel
- Információbiztonság (information security): az informatikai biztonságnál szélesebb, a szóban, írásban, az informatikai rendszerekben, vagy bármilyen más módon információk védelmére vonatkozik
- Információbiztonsági intézkedések:
    - Adatvédelem (data protection): a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége. (NAIH - Nemzeti Adatvédelmi és Információszabadság Hatóság)
    - Adatbiztonság (data security): Az informatikai biztonság részhalmaza, az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere. (NAIH)

Biztonsági célok – CIA hármas

- Bizalmasság(Confidentiality) Titkos vagy személyes információk (privacy) nem kerülhetnek jogosulatlanok kezébe. A bizalmasságot az adatok tárolásánál, feldolgozásánál és továbbításánál is garantálni kell.
- Sértetlenség(Integrity) Két fogalom: Adatintegritás (data integrity): Teljesülésekor az adat jogosulatlanul nem módosult tárolása, feldolgozása vagy küldése során.
- Rendszer sértetlensége (system integrity): A rendszer működése az elvártnak megfelelő, jogosulatlan módosításoktól mentes. Rendelkezésre állás(Availability) Biztosítja, hogy a szolgáltatás az arra jogosultak számára a szükséges időben és időtartamra használható.

További biztonsági célok

- Nyomon követhetőség (Accountability) Az a tulajdonság, hogy egy entitás által végrehajtott tevékenység visszakövethető legyen az entitáshoz. A tevékenységek ellenőrzés céljára rögzítésre kerülnek azért, hogy visszakövethetőek legyenek, bizonyíték álljon rendelkezésre. Ez a tulajdonság lehetővé teszi a letagadhatatlanságot (non-repudiation), a behatolások (intrusion) detektálását, megelőzését.
- Garancia, biztosíték (Assurance) A bizalom abban, hogy a négy másik biztonsági célt (bizalmasság, sértetlenség, rendelkezésre állás, számonkérhetőség) a biztonsági alrendszer megfelelően ellátja/eléri.

Fogalmak közötti kapcsolatok

- Bizalmasság függ a sértetlenségtől: Ha a rendszer sértetlensége sérült, akkor nem várható el, hogy a bizalmas adatok titkoban maradtak.
- Sértetlenség függ a bizalmasságtól: Ha bizonyos információ (pl. jelszó) bizalmassága sérül, a sértetlenséget biztosító mechanizmusok kikerülhetőek.
- Rendelkezésre állás és számonkérhetőség függ a bizalmasságtól: Ha bizonyos információ (pl. jelszó) bizalmassága sérül, a rendelkezésre állást és számonkérhetőséget biztosító mechanizmusok kikerülhetőek.
- Rendelkezésre állás és számonkérhetőség függ a sértetlenségtől: Ha a rendszer sértetlensége sérült, akkor a rendelkezésre állást és számonkérhetőséget biztosító mechanizmusok szabályos működése is sérülhetett.

Hitelesség

Hitelesség (Authenticity) 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 hitelesítéső kód (Message Authentication Code): Egy rövid, fix hosszúságú érték, mely lehetővé teszi az üzenet sértetlenségének és forrásának ellenőrzését, de nem biztosítja a letagadhatatlanságot

Sérülési szintek

Három szintet különböztetünk meg attól függően, hogy milyen fokú sérülés történik szervezeti, illetve személyi szinten.

- Alacsony: A sérülésnek csak korlátozott hatása van a szervezet, illetve a személy tulajdonára. A szervezet képes legfőbb feladatait végrehajtani, csak minimális kár keletkezik vagyontárgyaiban, bevétele csak minimális csökken, minimális személyi sérülés történik.
- Közepes: A sérülésnek komoly hatása van a szervezet, személy tevékenységére, tulajdonára. A sérülés jelentős kárt, bevétel csökkenést okoz, a szervezet még képes ellátni legfőbb feladatát, de hatásfoka jelentősen csökken.
- Magas: A sérülésnek végzetes hatása van a szervezet, személy tevékenységére, tulajdonára. Katasztrofális kár történik a vagyontárgyakban, tragikus költséget, személyi sérülést okoz, a szervezet nem képes ellátni feladait.

Fizikai védelem

A fizikai védelem feladata azon fizikai erőforrások védelme, melyek az adatok tárolását, feldolgozását, továbbítását biztosítják. A védelmi intézkedések többsége preventív vagy detektív.
Fizikai infrastruktúra (általános fogalom):

- Informatikai rendszer hardver elemei: Adatfeldolgozó és tároló eszközök, adatátviteli és hálózati elemek és oine tároló eszközök. Ide soroljuk az informatikai rendszer dokumentációit is.
- Épületek: Épületek, ahol az informatikai rendszer fizikai elemei megtalálhatóak.
- Kiszolgáló rendszerek: Elektromos vezetékek, kommunikációs hálózatok,víz- és gázvezetékek.
- Személyzet: Azon személyek, melyek az informatikai rendszer használói, fenntartói vagy működtetői.

Fizikai fenyegetések kategóriái

- Környezeti fenyegetések, természeti csapások
- Technikai fenyegetések
- Emberi fenyegetések

Természeti csapások

- Tornádó forgószél, Trópusi ciklonok hurrikánok, trópusi viharok, tájfunok
- Földrengés
- Jégvihar
- Villám
- Árvíz

Technikai fenyegetések

Olyan környezeti feltételek, melyek korlátozzák vagy megszakítják az informatikai rendszer szolgáltatását, vagy a tárolt adatokat

Nem megfelelő hőmérséklet

- A legtöbb számítógépes rendszert 10 és 32 fok közötti hőmérsékleten kell tárolni.
- Ezen az intervallumon kívül az erőforrás továbbra működőképes, de lehet, hogy nem megfelelő eredményeket ad.
- Ha a környezet hőmérséklete nagyon magas lesz, a számítógép nem lesz képes megfelelően hűteni magát és a belső komponensek sérülhetnek.
- Ha a hőmérséklet túl alacsony, bekapcsolásnál a rendszer hőtani sokkon esik át, mely integrált áramkörök sérüléséhez vezethet.
- Okostelefonok, digitális kamerák, táblagépek és laptopok stb. akkumulátorainak kapacitása is csökken, ha túl meleg vagy túl hideg van.

Az eszköz belső hőmérséklete

- A belső hőmérséklet jelentősen nagyobb, mint a szoba hőmérséklete.
- Saját hűtésük külső feltételektől is függ: pl. külső hűtés léte

Magas páratartalom

- A hidegből a meleg épületbe érve sincsenek azonnal biztonságban az eszközök, ekkor ugyanis pára csapódhat le a belsejükben. Magas pára korróziót okozhat.
- A vízcseppek zárlatot okozhatnak az alkatrészekben pl. mágneses és optikai tárolókat (vízálló táblagépek és okostelefonok)

Statikus elektromosság

- A sztatikusan feltöltött személyek, tárgyak kárt okozhatnak az elektromos eszközökben.
- Már a 10 voltos kisülések is kárt okozhatnak az áramkörökben.
- Több száz voltos kisülések jelentős kárt okozhatnak.
- Az emberi test jóval több elektromos ellenállás tárolására alkalmas, mint egy átlagos IC. Az emberi sztatikus kisülések több ezer voltot is elérhetik.

Tűz, füst

- emberi életre és a berendezésekre is vonatkozó fenyegetés
- a közvetlen láng és a hő is veszélyforrás
- mérgező gázok felszabadulása veszélyes az emberekre nézve
- tűzoltásból keletkező vízkár, füstkár

Víz

- a számítógépes eszközöket, papírokat, elektromos tároló eszközöket veszélyezteti
- elektromos rövidzárlat keletkezhet

Por

- Általában ezzel a fenyegetéssel kevésbé foglalkozunk.
- Szellőzőréseken át bejutó por eltömíti a levegő szabad áramlásának útját, ezért a belső ventilátor nem tudja kellő hatékonysággal hűteni a működése során forróvá váló processzort.

Rovarfertőzés

Feszültséghiány

- A berendezés kevesebb feszültséget kap, mint amennyire szüksége van a normál működéshez.
- A legtöbb számítógép ellenáll a kb. 20%-os feszültséghiánynak, még nem áll le, nem történik működésbeli hiba.
- Nagyobb feszütséghiány leállítja a rendszert.
- Komolyabb kár sérülés nem keletkezik, csak a szolgáltatás szakad meg.

Túlfeszültség

- áramszolgáltatási anomáliák, villámcsapás okozhatja
- processzorokban, memóriákban okozhat kárt

Elektromágneses Interferencia

- Elektromos eszközök, más számítógépek elektromos zajt generálnak, mely kárt okozhat a saját számítógépünkben.
- Ez a zaj a térben és elektromos vezetékeken is továbbítódik.
- Zaj eredhet a közeli mikrohullámú antenna, vagy akár mobiltelefon révén is.

Emberi fizikai fenyegetések

Az emberi zikai fenyegetések kevésbé kiszámíthatóak, mint más zikai fenyegetések. Az emberek a rendszer leggyengébb pontjait keresik.

- Jogosulatlan zikai hozzáférés: Szerverek általában lezárt területen vannak, ahova való bejutás korlátozott. Néhány alkalmazottnak van jogosultsága. Jogosulatlan zikai hozzáférés lopáshoz, vandalizmushoz és visszaéléshez vezethet.
- Lopás: berendezések eltulajdonítása, adatok megszerzése csatorna lehallgatása is ide tarozik
- Vandalizmus: berendezések tönkretevése
- Visszaélés: az erőforrások jogosulatlan használata

Fizikai preventív kontrollok

Általános preventív védekezés: felhők használata

- lokálisan lényegesen kevesebb erőforrásra van szükség

- a nagy mennyiségű adatok lokálisan nincsennek zikai fenyegetéseknek kitéve

Környezeti fenyegetések

- Nem megfelelő hőmérséklet és páratartalom: Mérőeszközök segítségével a megfelelő környezetet el lehet érni. Ha az érték túllép a megengedett határon, akkor jelez is.
- Vízkár: Vízérzékelők elhelyezése a padlón és az emelt padlók alatt. Víz esetén automatikusan le kell, hogy kapcsolódjon az áram.
- Por: Ventillátor szűrő karbantartása és a helyiség tisztán tartása.
- Tűz, füst: Tűzjelzők, megelőző intézkedések, tűz oltása Ritkán keletkezik katasztrófális tűz egy jól védett számítógépes helyiségben. Úgy kell a helyiséget kiválasztani, hogy minimális legyen a környezetében keletkező tűz, víz, füst kockázata. Védelmi intézkedések: Közös falak legalább egy óra hosszat tűzálló legyenek. Légkondicionállók úgy legyenek megtervezve, hogy a tüzet ne terjesszék. Gyúlékony anyagokat ne tároljunk a helyiségben. Kézi tűzoltókészülék legyen elérhető, egyértelműen jelezve, és rendszeresen tesztelt. Automata tűzoltó rendszer is legyen telepítve. Tűzjelzők vészjelet adjanak le a helyiségben és külső felügyeletnek is. Főkapcsoló szükséges és egyértelműen jelezve legyen. Menekülési útvonalak ki legyen függesztve. Fontos adatok, dokumentumok tűzálló kabinetben legyenek. Az adatok, programok up-to-date másolata más helyiségben legyen. Biztosítási cégek, tűzoltóság vizsgálja át az épületet.
- Elektromos teljesítmény, Elektromágneses interferencia: Szünetmentes tápegység kapcsolása minden egyes kritikus berendezéshez. Szünetmentes tápegység elektromos áramot biztosít, ha megszűnik a hálózati áramforrás, áramingadozás van, vagy áramszünet lép föl. A szünetmentes tápegység áthidalási ideje néhány perctől pár óráig terjed. Hosszabb kimaradások esetén generátor szükséges.

Emberi fenyegetések

- Csak az arra jogosult léphet be az épületbe. Nem vonatkozik az alkalmazottakra, jogosulatlan belső támadókra.
- Erőforrásokat tegyük zárható tárolókba, széfekbe, szobákba.
- Berendezéseket rögzítsük olyan tárgyakhoz, melyeket nem lehet elmozdítani.
- Mozdítható berendezéseket nyomkövetővel láthatunk el, mely jelzi, ha elhagyja a területet.
- Hordozható eszközök nyomkövetővel való ellátása, mely állandó monitorozást tesz lehetővé.
- A megfigyelő rendszer része az épületnek. Ezek a rendszerek valós idejű távoli megfigyelést és rögzítést jelent.

Fizikai helyreállító kontroll

A helyreállító kontroll hasonlít a korrektív kontrollhoz, csak komolyabb helyzetekben alkalmazzuk.

- A legfontosabb helyreállító intézkedés a másolatok készítése: Backups.
- A másolatok nem védenek az esetleges bizalmassági sérülésekkel szemben, de az adatok visszaállíthatóak.
- Hot site: Közel valós idejű szinkronizálással készített másolat, mely képes egyből átvenni a szolgáltatást.
- A víz, a füst, a tűz maga után hagy maradványokat, melyeket el kell takarítani. Speciális tisztítókat kell hívni.

Titkosítási sémákról általában

Szimmetrikus titkosítási sémák

- A titkosító és visszafejtő kulcs megegyezik, vagy a visszafejtő a titkosító kulcsból könnyen (polinomiális időn belül) kiszámítható.

Aszimmetrikus titkosítási sémák

- A titkosító és visszafejtő kulcs különbözik olyannyira, hogy a visszafejtő a titkosító kulcsból csak nehezen (nem ismerünk rá polinomiális idejű algoritmust) számítható ki.

Szimmetrikus titkosítási séma formális definíció

A SE = (Key, Enc, Dec) hármas egy szimmetrikus titkosítási séma, ha

- Key: kulcsgeneráló algoritmus, mely egy k biztonsági paraméterhez (kulcs méretére utal) megad egy K ∈ K titkos kulcsot.
- Enc: titkosító algoritmus, mely ∀m ∈ P nyílt üzenethez és ∀K ∈ K titkos kulcshoz generál egy c ∈ C titkosított üzenetet. $c = Enc_k(m)$
- Dec: visszafejtő algoritmus, mely egy c ∈ C titkosított üzenethez és egy adott K ∈ K kulcshoz megad egy m ∈ P nyílt üzenetet. $m = Dec_k(c)$
- Sok esetben a titkosítási algoritmus inputja egy r véletlen is. Így a titkosító algoritmus randomizált.
- A visszafejtő algoritmus determinisztikus.
- Definíció: Az SE = (Key, Enc, Dec) szimmetrikus titkosítási séma korrekt visszafejtést biztosít, ha ∀m ∈ P és ∀K ∈ K esetén $Dec_k(Enc_k(m)) = m$.

Aszimmetrikus titkosítási séma formális definíció

A AE = (Key, Enc, Dec) hármas egy aszimmetrikus titkosítási séma, ha

- Key: kulcsgeneráló algoritmus, mely egy k biztonsági paraméterhez (kulcs méretére utal) megad egy (PK, SK) ∈ K nyilvános és titkos kulcsból álló párt.
- Enc: titkosító algoritmus, mely ∀m ∈ P nyílt üzenethez és PK nyilvános kulcshoz generál egy c ∈ C titkosított üzenetet. $c = EncP_k(m)$
- Dec: visszafejtő algoritmus, mely egy c ∈ C titkosított üzenethez és egy adott SK kulcshoz megad egy m ∈ P nyílt üzenetet. $m = DecS_k(c)$
- Sok esetben a titkosítási algoritmus inputja egy r véletlen is. Így a titkosító algoritmus randomizált.
- A visszafejtő algoritmus determinisztikus.
- A kulcsgeneráló algoritmus outputja meghatározza a P, C, K halmazokat.
- Definíció: Az AE = (Key, Enc, Dec) aszimmetrikus titkosítási séma korrekt visszafejtést biztosít, ha ∀m ∈ P és ∀(PK, SK) ∈ K esetén $DecS_k(EncP_k(m)) = m$.

HASH függvények

Kriptográfiai hash függvények

Definíció: A $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$, n ∈ N függvényt hash függvénynek nevezzük.

Tetszőleges véges hosszú üzenethez n hosszú üzenetet rendelünk.

- pl.: MD5, SHA-1, SHA-256, SHA-512, SHA-3(Keccak, 2015)
- adatintegritás ellenőrzése: Hash függvénnyel ellenőrizhetjük, hogy egy állomány változott -e vagy sem. Az állomány hash értéke szeparáltan tárolt. Kiszámítjuk az állomány hash értékét és összevetjük a tárolt hash értékkel. Ha különböznek, akkor az állomány módosult.
- A hash értéket lenyomatnak is hívjuk.
- lavinahatás: Egy bit változása az inputban, jelentős változást eredményez az outputban. (pl. az output fele)

Elvárások

- A hash fügvények nem injektívek
- Definíció: Az $(x, x') \in \{0, 1\}^* \times \{0, 1\}^*$ a H hash függvény egy ütközése, ha x != x ’ és h(x) = h(x ’).
- Három jellemző:
- 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 != x ’ és H(x) = H(x ’).
- Ütközésmentes(erősen ütközésmentes): Nehéz olyan x, x’ ∈ X értékeket találni, hogy H(x) = H(x’).

Üzenethitelesítés – Message Authentication Codes (MAC)

Jellemzők:

- Hitelesség (forrása az, amit megjelöltek, adatintegritás)

Digitális aláírási sémák

- Biztonsági jellemzők:
- Hitelesség (forrása az, amit megjelöltek, adatintegritás)
- Letagadhatatlanság

Formális definíció:
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 $s = Sign_{sk}(m)$ 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.
- M üzenetek halmaza, S az aláírások halmaza

Támadó célja:

- Teljes feltörés: A támadó ki tudja számolni az aláíró fél titkos kulcsát.
- Univerzális hamisítás: A támadó bármilyen üzenethez képes érvényes aláírást generálni.
- Szelektív hamisítás: A támadó képes egy általa választott üzenethez aláírást generálni.
- Egzisztenciális hamisítás: A támadó képes egy aláírt üzenetet generálni.

Támadási módok:

- Csak a nyilvános kulcs ismert (Key-only attack): A támadó csak a nyilvános kulcsot ismeri.
- Ismert üzenet alapú támadás (Known message attack): A támadó ismer egy ugyanazon kulccsal aláírt üzenetlistát.
- Választott üzenet alapú támadás (Chosen message attack): A támadó rendelkezésére áll egy általa választott üzenetek és a hozzájuk tartozó aláírások listája.
- Adaptívan választott üzenet alapú támadás (Adaptive chosen message attack): A támadó rendelkezésére áll egy általa választott üzenetek és a hozzájuk tartozó aláírások listája, ahol az üzenetet a korábban megkapott aláírások alapjám választja ki.

RSA titkosítás

1977-ben jelent meg
Tervezői: Ron Rivest, Adi Shamir, és Leonard Adleman
Legtöbb Nyilvános Kulcs Infrastruktúra (PKI) termékben megtalálható, SSL/TLS tanúsítványok
Biztonságos e-mail: PGP, Outlook

Aszimmetrikus titkosítási séma: $AE = (Key, Enc, Dec)$

- *Key*:
  1. Véletlenül választunk két nagy prímet: p, q.
  2. Kiszámítjuk az RSA modulust: $n = p \cdot q$.
  3. Kiszámítjuk az Euler-féle ϕ függvényt: $\phi(n) = (p-1)(q-1)$.
  4. Választunk egy *véletlen* e egészt: $1 < e < \phi(n)$ és $(e, \phi(n)) = 1$. (e titkosító kitevő)
  5. Kiszámítjuk d-t: $1 < d < \phi(n)$ és $ed \equiv 1 \pmod{\phi(n)}$. ($d$ visszafejtő kitevő)

  $PK = (n, e)$, $SK = d$ and $\phi(n), p, q$ titkos paraméterek
  $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$
- $Enc_{PK}(m) = m^e \pmod{n}$ $\forall m \in \mathcal{P}$ és $PK = (n, e)$ mellett.
- $Dec_{SK}(c) = c^d \pmod{n}$ $\forall c \in \mathcal{C}$ és $SK = d$ mellett.

- *Key*:
  1. Véletlenül választunk két nagy prímet: p, q. -> **Prímtesztek** (pl. Miller-Rabin prímteszt)
  2. Választunk egy *véletlen* e egészt: $1 < e < \phi(n)$ és $(e, \phi(n)) = 1$. -> **Euklideszi algoritmus**
  3. Kiszámítjuk d-t: $1 < d < \phi(n)$ és $ed \equiv 1 \pmod{\phi(n)}$. -> multiplikatív inverz számítása: **Kibővített Euklideszi Algoritmus**
- $Enc_{PK}(m) = m^e \pmod{n}$ $\forall m \in \mathcal{P}$ és $PK = (n, e)$ mellett. -> **Gyors hatványozás**
- $Dec_{SK}(c) = c^d \pmod{n}$ $\forall c \in \mathcal{C}$ és $SK = d$ mellett. -> **Kínai Maradéktétel alkalmazása**

AES:

Rijndael: Joan Daemen, Vincent Rijmen

- $SE = (Key, Enc, Dec)$ szimmetrikus titkosítási séma
- $\mathcal{P} = \{0,1\}^{128}$
- $\mathcal{C} = \{0,1\}^{128}$
- $\mathcal{K} = \{0,1\}^k$, $k \in \{128, 192, 256\}$
- *Key*: véletlenül választunk egy $K \in \mathcal{K}$

AES animáció!

- Egy kör: SubByte, ShiftRow, MixColumn, AddRoundkey
- Körök száma: $\begin{cases} k = 128, & 10; \\ k = 196, & 12; \\ k = 256, & 14. \end{cases}$