Az elektronikus kereskedelem kifejezései

A

Access card: (hozzáférést biztosító kártya) Géppel olvasható kártya, amit számítógépes bejelentkezéshez, fizikai beléptetéshez, ill. áthaladáshoz használnak.
Access control: (hozzáférés ellenőrzése) Intézkedés, ami biztosítja, hogy egy forrás csak a jogosult számára legyen elérhető.
Acquirer: (elfogadó) Intézmény, például bank, aminek szerződéses megállapodása van kereskedőkkel, abból a célból, hogy elfogadjanak bankkártyákat áruk és szolgáltatások ellenértékének kifizetéséhez, ill. kereskedői készpénzfelvételhez. Az elfogadó megtéríti a kereskedőnek a tranzakciók értékét, és jutalékot számít fel a szolgáltatásért. Ez az intézmény üzemelteti a terminálokat, amikről a tranzakciók származnak.
Ad View (Ad Impression): A Page Impression egy speciális formája, amely a Banner reklámokat számolja. Mivel sok oldal állandóan cserélődő (rotáló) Bannerekkel dolgozik, így a hirdetőnek csak azok a letöltések (Page Impression-ök) számítanak, amelyeken az ő hirdetése is megjelent.
Adat: Az információ nem értelmezett, de értelmezhető formája
ADS: Automated debiting systems (automatikus terhelési rendszerek) EC project, célja csökkenteni az autópályák forgalmát.
AES (Advanced Encryption Standard): 1997-ben pályázatot írtak ki a DES leváltására. Erre több pályázat is érkezett, de a válogatás és a különböző megmérettetések még tartanak. A kiírásnak nem célja hogy alapot keressenek a jövő titkosításához. A jövőbeli győztes algoritmust pedig AES-nek keresztelték.
AFC: Automatic fare collection (automatikus utazási díjbeszedés) érintkezéses, vagy érintkezés nélküli chipkártyás közlekedési rendszereknél.
algorithm: (algoritmus) Matematikai műveletsor, amit például adatok titkosítására és visszafejtésére alkalmaznak.
Alkalmazásszűrő: Alkalmazásvizsgáló tűzfalfajta a rendszerben megengedett lakalmazások futását figyeli, a nem megengedett alkalmazást nem futhatathatunk.
Alpha test: (alfa teszt) Egy új program, rendszer, vagy hardware kezdeti próbafuttatása a fejlesztő szervezeten belül. (Lásd még béta teszt.)
American National Standards Institute: A Nemzetközi Szabványügyi Szervezet tagtestülete az USA-ban.
ARP - Address Resoultion Protocol: cím visszafejtő protokoll, segítségével végzik a lokális hálózaton a berendezések IP számainak azonosítását. Egy ARP kérésre az adott IP-vel rendelkező gép visszaadja saját MAC címét, mellyel a LAN-on az adatok továbbítása megvalósulhat.
ARPA - Advanced Research Projects Agency: Az USA Hadügyminisztérium 1957-ben alapított fejlesztési szervezete. Több alkalommal DARPA névre változtatták.
ARPANET - Az INTERNET elődje, fejleszté-sét az ARPA kezdeményezte és finanszí-rozta.
artifical intelligence: (mesterséges intelligencia) Információfeldolgozás az agyi, idegi vagy kognitív folyamatok utánzása, vagy szimulálása révén.
ASCII: American Standard Code for Information Interchange. (Amerikai szabványkód az információ cseréhez, az írásjelek egyik legrégebben és legelterjedtebben használt kódolása az ember-gép kapcsolatban.) A legtöbb PC által használt protokoll, ami 7-bites kódot rendel 96 nyomtatható karakterhez és 32 ellenőrző karakterhez.
Association for Payment Clearing Services (APACS): Az Egyesült Királyság fizetési iparágát összefogó szervezet.
Aszinkron átvitel: Olyan távközlési csatorna üzemmódja, amelyben az adó- és a vevőoldal együttfutását nem biztosítják speciális időzítési információk, hanem minden adategység elejét és végét ún. start- és stopbitek jelzik.
Asymmetric key cryptography: (aszimmetrikus kulcsú titkosítás): Biztonsági rendszer, ahol a

titkosításhoz és visszafejtéshez használt kulcs különböző. Van nyilvános kulcs (public key) és saját kulcs (private key). Mindkét kulcs alkalmas titkosításra. Amit a privát kulccsal titkosítanak, az a hozzá tartozó publikus kulccsal fejthető meg (ha azoknak akarok üzenni, akik rendelkeznek az én publikus kulcsommal). Amit a publikus kulccsal titkosítanak az a hozzá tartozó privát kulccsal fejthető meg (valakinek üzenni akarok, és azt akarom, hogy csak ő olvashassa el).
Asynchronous: (aszinkron): Nem szinkron. A leggyakoribb adattovábbító módszer PC-knél.
Aszimmetrikus kulcs: lásd nyilvános
ATM: Asynchronous Transfer Mode: (aszinkron adattovábbítási mód) új kommunikációs protokoll mindenféle adat továbbítására hálózaton keresztül. Nagy sebességű adatátviteli megoldás. Az információt igen kis (53 byte-os) egységekre bontva kezeli.
ATM: Automated Teller Machine, bankjegykiadó automata
Audit Trail: (eseménynapló): Napló, ami minden eseményt időrendben rögzít és biztonsági célból felhasználható.
Audit/journal printer: (ellenőrző/naplózó nyomtató) Nyomtató, ami minden eseményt megtörténtekor rögzít, és auditálási lehetőséget nyújt.
Authenticate: (hitelesítés) Személyazonosság vagy eredet biztosítására.
Authentication routine: (hitelesítő eljárás) Egy folyamat a felhasználó, a kártya, a terminál, vagy az üzenettartalom ellenőrzésére. A "kézfogásként" (handshake) is ismert hitelesítés fontos adatokat használ a kód előállítására, amit real time vagy batch feldolgozással ellenőriznek.
Authorisation code: (engedélyezés kódja) A tranzakcióhoz rendelt engedélyezési kód, ami lehetővé teszi az érvényes engedélyezés igazolását.
Authorisation message: (engedélyező üzenet) A fizetési rendszeren belüli olyan üzenet a kártyakibocsátó és az elfogadó között, ami arra szolgál, hogy megállapításra kerüljön, hogy a kibocsátó jóváhagyja-e a tranzakciót.
Authorisation terminal: (engedélyező terminál) Egy terminál, ami a tranzakciót engedélyezi, de nem feltétlenül gyűjti be a tranzakciós adatokat a fizetési rendszer számára.
Authorisation: (engedélyezés) A tranzakciós kérés elutasítása, vagy jóváhagyása. A kártyakibocsátó az engedélyezéssel vállalja, hogy kifizeti a kártyaelfogadónak a tranzakció összegét.
Automated Clearing House: (Automatikus Klíring Ház) Pénzügyi intézmények közötti és vállalatok közötti pénz átutalások, állami értékpapír ügyletek elektronikus feldolgozását végzi.
Automated teller machine: (bankjegykiadó automata) Számítógépesített önkiszolgáló eszköz, mely feljogosít a megfelelő kártya és PIN kód birtokában számláról való pénzfelvételre, és egyéb banki szolgáltatások igénybevételére. Cash dispenser (készpénzadagoló) néven is ismert.

B

B2A: Business to Administration: Az elektronikus kereskedelem egyik típusa, amikor az elektronikus úton létrejött üzlet az üzleti élet egyik szereplője és a kormányzat között történik, a közigazgatás és az üzleti szektor közötti ügyleteket foglalja magában. A B2B részterülete is lehet , ahol a az egyik fél mindig valamilyen közigazgatási szerv.
B2B Business to Business: Az elektronikus kereskedelem egyik típusa, amikor az elektronikus úton létrejött üzlet az üzleti élet két szereplője között történik. Pl. GE és a beszállítói között. Olyan gazdasági kapcsolat, amelyben valamennyi résztvevő az üzleti szektorból kerül ki. Kereskedelmi rendszereket, módszereket igényel, amelyek az elektronikus üzletet lehetővé teszik. Forradalmasítja a beszállítói láncot, illetve az ügyfél- partner-kapcsolatokat.
B2C Business to Consumer: Az elektronikus kereskedelem egyik típusa, amikor az elektronikus úton létrejött üzlet az üzleti élet egyik szereplője és egy magánszemély között történik. Pl. az amazon.com internetes áruházban. Az üzleti szereplő által megcélzott fél a fogyasztó. A hétköznapi vásárlás elektronikus formája.
Bank card: (bankkártya) A bankkártya szabványos méretű, általában bankszámlához kapcsolódó

műanyag kártya, ami áruk és szolgáltatások ellenértékének kiegyenlítésekor készpénzkímélő fizetési eszközként és/vagy készpénzfelvételre és/vagy ügyfél-azonosításra használható az engedélyezett régióban, az engedélyezett környezetben (elektronikus vagy nem csak elektronikus).
Banner (Szalaghirdetés) – Az internetes reklámozás legáltalánosabban használt eszköze. Mérete 468*60 pixel. Az IAB/CASIE szabvány szerint ez a "full banner", más méreteket (lásd pl: button) külön névvel láttak el.
Banner burnout - Banner kiégés. A Bannerekre való rákattintások csökkenő arányát jelenti, míg az internetes reklámozás kezdetén (1994) 10-20%-os volt 2000-re mintegy 0,3-0,4%-ra süllyedt (USA). A CTR csökkenése az egyes kampányok során is előfordulhat.
Batch processing: (kötegelt feldolgozás) Az adatfeldolgozás módja, amikor az adatokat egy időtartamig későbbi kötegelt feldolgozás céljából gyűjtik.
Baud - A távközlési csatorna másodpercenkénti jeleinek egysége, azaz a jelsebesség mértéke. Azt mutatja meg, hogy másodpercenként hányszor változik meg a csatorna állapota a moduláció következtében. A moduláció típusától függően az adatátvitel sebessége ennek többszöröse lehet.
BBS - Bulletin Board System: – Elektronikus hirdetőtábla. Az egyik legrégibb elektronikus kommunikációs rendszer, amelyen üzeneteket, információkat lehet cserélni. A BBS-ek kiegészítő szolgáltatásként elektronikus levelezést, letölthető szoftverkönyvtárakat, kereső szolgáltatásokat stb. üze-meltetnek. Interaktív szolgáltatás.
Behatolás-figyelő: A rendszerben történő külső behatolást figyeli és különböző 'jelekből' megállapítja mi történt, ki volt a tettes és kitiltja a kapcsolatot.
beta test: (béta teszt) Egy új program, rendszer, vagy hardver első nyilvános tesztje a kiválasztott felhasználók között, ellenőrzött körülmények mellett. Lásd még: alpha test
binary: (kettes számrendszer) Csak a 0 és 1 értékeket használja.
biochip: Szintetizált szerves molekulákból készített chip, mely nagy mennyiségű felhasználásra készül különlegesen gyors számítógépekhez. 1000-szer gyorsabbnak tartják a szilikon chip-nél és 100,000-szer kevesebb áramot fogyasztanak.
Biometric authentication: (biometrikus hitelesítés) Egy személy azonosságának ellenőrzésére szolgáló módszer, aminek során személyes biológiai jellemzőket vizsgálnak (pl.: ujjlenyomat, retinaolvasás, írisz- vagy hangvizsgálat).
Bit rate: (bit továbbítás sebessége) Az információtovábbítás sebessége kommunikációs csatornában, bit/mpben kifejezve.
Bit: BInary digiT - Az információ egysége a kettes alapú számrendszerben 0, 1. A legkisebb lehetséges digitális információs kódegység.
Biztonság (security): Kontrolálatlan veszteségek és hatások elleni védelem állapota illetve ennek minősége. Abszolút biztonságot tulajdonképpen lehetetlen elérni; azaz a biztonság relatív fogalom. Már csak azért is, mert a felhasználók nem költenek többet a biztonsági rendszerekre, mint amit a védendő információ ér. Másrészről biztonságtechnikai szakemberek körében is elfogadott az a kijelentés, miszerint a végtelen (tökéletes) biztonságnak végtelen ára van.
Blowfish: Szimmetrikus rejtjelező, blokk-rejtjelező. A 3DES-hez hasonlóan a sima DES-nél jóval biztonságosabb. Bruce Schneier "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)" 1993-as munkájában jelentette meg.
bps: bit/másodperc Egy másodperc alatt továbbított bitek számát kifejező mértékegység.
bridge: (híd) Egy eszköz, amivel össze lehet illeszteni különböző kommunikációs áramköröket egymással, jelcsere elősegítése céljából.
Browser (Böngésző): A WWW grafikus felületének megjelenítésére szolgáló, helyi platformon üzemelő szoftver.
Browser: A World WideWeb és más internetforrások elérését segítő program (a legismertebbek az Internet Explorer és a Netscape Communicator).
BSI: British Standards Institution (Angol Szabványügyi Testület)
bus: Útvonal rézfólia vonal formában, amin keresztül az adat az áramköri lapon közlekedik. Az átkapcsolást vagy a kapcsoló (dipswitch) végzi az eszközön, vagy egy szoftver.
Button (Gomb): A Bannernél kisebb reklám, leginkább 120*90, 120*60, 125*125, 88*31 pixel

méretben.
byte: 8 bit sorozata, amit általában egy egységként működtetnek.

C

C2A Consumer to Admionistration: A közigazgatás és magánszemélyek közötti elektronikus ügyletek elnevezése.
C2A Consumer to Admionistration: A közigazgatás és magánszemélyek közötti elektronikus ügyletek elnevezése.
C2C Consumer to Consumer: A fogyasztók egymás közötti elektromos kommunikációját jelzi.
C2C Consumer to Consumer: A fogyasztók egymás közötti elektromos kommunikációját jelzi.
CAD: computer-aided design
CAM: Card Authentication Method. Kártyahitelesítő módszer.
CCITT - Comité Consultatif International Téléphonique et Télégraphique, International Telegraph and Telephone Consultative Committee, utódja az ITU-T – Genfi székhelyű nemzetközi tanácskozó testület a vezetékes távközlés kérdéseiben.
CD - Compact Disk: Eredetileg archivált hangfelvételek (vö. Compact Cassette), majd filmek, szoftverek kereskedelmi forgalmában terjedt el.
CD ROM (Compact Disk-Read Only Memory): Csak olvasható (ROM) információ, amit CD-ről töltenek be a számítógépre. Nagymennyiségű (650 MB) multimédia-információ utólag meg nem változtatható optikai tárolását lehetővé tevő 12 cm átmérőjű lemez. Hosszú élettartamú, korlátlanul olvasható a speciális meghajtókban.
CEC (chip electronic commerce): Az EMVCo által kifejlesztett chip alapú elektronikus kereskedelem specifikáció, amely azzal foglalkozik, hogy hogyan lehet az EMV szabványú intelligens kártyákat biztonságos fizetőeszközként felhasználni az interneten.
CEPS: Common Electronic Purse Specification (Közös Elektronikus Pénztárca Specifikáció). 1998 júniusában készítették abból a célból, hogy meghatározza az elektronikus pénztárcarendszerek iránti követelményeket.
certification authority (CA): (hitelesítő hatóság) Megbízott harmadik fél, aki olyan bizonyítékot állít elő, ami egy nyilvános kulcshoz és más kapcsolódó információhoz hozzákapcsolja a tulajdonosát.
CGI - Common Gateway Interface: A CGI-t támogató böngészőprogramok szabványos módon teszik elérhetővé futtatható programok weblapokhoz csatolását. A futtatható program a legkülönbözőbb dolgokat végezheti, a weblap-számlálótól az adatbázis-kezelésig rengeteg alkalmazása lehetséges.
chip card: chip kártya. (=integrated circuit card, IC Card, microprocessor card, smart card) Olyan kártya, amely adatokat tárol a kártyába beültetett számítógép chipben. A chip az adatokat fel tudja dolgozni, és el is tudja tárolni. Ilyen kártyákat használnak bankkártyákhoz, GSM telefonokhoz, igazolványokhoz, parkolókhoz, bónuszkártyákhoz, és titkosítókártyákhoz is. Lásd még smart card.
chip: szilíciumdarab elektronikus áramkörrel bemetszve.
CKS: (Checksum) Ellenőrző összeg: ellenőrző eljárás valamely művelet végrehajtásának ellenőrzésére.
Click Through (Átkattintás): Egy átkattintás egy Link vagy egy Banner tényleges aktiválását fejezi ki, azt jelenti, hogy a látogató valóban elugrik a linkelt oldalra.
Click-Through Rate (CTR, Átkattintási ráta): Azt az arányt fejezi ki, ami egy Banner megjelenési gyakorisága és a rákattintások gyakorisága között van. A CTR vagy 20:1 formában van megadva (egy a 20 látogatóból kattintott a Bannerre), vagy százalékban pl. 5%.
CMR - Commercial Mail Relay – Az Internet-levelezés egyik első kereskedelmi átjárója.
connectivity: Az adatfeldolgozó rendszerek azon képessége, vagy funkciója, hogy egymással összekapcsolódjanak és együttműködjenek.

Conversion event (Konverziós esemény) – Minden olyan esemény, amit a hirdető lényegesnek ítél az online vásárlás szempontjából (pl. a látogató betesz valamit a kosárba, vagy megrendel valamit, vagy kifizeti az árut stb.)
Cookie: Egy olyan kódszám, amit egy Website számítógépe küld a felhasználó számítógépének, hogy azt a gép későbbi azonosításának céljából tárolja.
Cost Per Click (CPC) – A CPM ár és az ezer Ad View-ra jutó kattintások számának hányadosa. Megmutatja, hogy a hirdetőnek egy Banner reklámmal elért, a Website-ra érkezett Látogató mennyibe kerül.
Cost Per Lead (CPL) – Egy Lead beszerzési költségét jelenti. (Az ezer hirdetés megjelenítési költségéből az Átkattintási és a Konverziós rátán keresztül számítható.)
Cost Per Thousand Impressions (CPM): Ezer kapcsolatra jutó - költség - a klasszikus reklámok esetében is használatos érték, mely ezer kapcsolatonként jelöli egy reklám költségeit. Az online reklám esetében ez az 1000 Ad View médiaköltségét jelenti.
cracker: Egy olyan személy, aki megpróbál engedély nélkül, rosszindulatúan számítógépes rendszereket elérni/feltörni. Számítógépes szakérő, rendszerekbe hatol be általában nyereségvágyból vagy információ szerzés céljából. (lásd még hacker) **credit card: (hitelkártya)** Fizetési kártya, ami lehetővé teszi a kártya birtokosának, hogy egy előre meghatározott hitelkeretig árukat és szolgáltatásokat vásároljon és készpénzt vegyen fel. A kártyabirtokos a kinnlevőségét egészben, vagy részben törleszthetí egy meghatározott időszak végén, vagy továbbgörgetheti a következő időszakra, amire hitelkamatot számítanak fel.
CRM (Customer Relationship Management): ügyfélkapcsolat menedzsment, vállalati szintű szoftver-alkalmazások együttese amely az ügyfélkapcsolatok minden vonatkozásáanak kezelését lehetővé teszi. (ezköze a központi adatbázis)
cryptanalysis: A titkosítás megfejtése az adatok elemzésével, anélkül hogy tudnánk a kulcsot, amivel a titkosítást végezték.
cryptography: (titkosítás) Bizalmas információk átalakításának módszere abból a célból, hogy illetéktelenek számára ne legyen érthető.
cryptosystem: Rendszer, ami titkosít és megfejt információkat.
CSA - Common Scrambling Algorithm: Adatvédelmi eljárás.
csomagszűrő: Olyan tűzfalfajta, ami a csomagokat vizsgálja és engedi meg a mozgásukat a rendszerbe vagy a rendszerből.
CUG - Closed User Group – Zárt előfizetői csoport.

D

Daemon: A kliens-szerver szoftverek szerver része. A unix környezetben használt daemon elnevezés azt a szoftvert jelenti ami vár egy kliens bejelentkezésére és kiszolgálja azt. A program elnevezésében a név végén levő d betűvel szokták megkülönböztetni a daemon programot a klienstől.
Data Encryption Algorithm (DES): (adat titkosító algoritmus) A Data Encryption Standard szabványban meghatározott titkosító algoritmus.
Data Encryption Standard (DES): (adattitkosító szabvány) Amerikai szabvány, ami meghatároz egy titkosítási rendszert az amerikai kormány számára. A DES néven ismert titkosítási rendszert a fizetési rendszerekben széles körűen használják. Ez a titkosító algoritmus egyetlen titkosító kulcsot használ. A titkosításimegfejtési módszer szimmetrikus, mert ugyanazt a kulcsot használják az adat titkosítására és megfejtésére.
data integrity: (adatsértetlenség) A sértetlen adatot nem módosították, vagy törölték engedélyezetlen módon.
data warehouse: (adatraktár) Széles körből összeszedett adatbázisokból álló "raktár" abból a célból, hogy további információszerzéshez elemezzék őket.
DCE - Data Circuit-Terminating Equipment: Adatátviteli berendezés, pl. modem.

DCE - Distributed Computing Environment: Elosztott informatikai rendszer.
DDP: distributed data processing
DEA: Data Encryption Algorithm
Dedicated network: (dedikált hálózat) Kommunikációs funkció, amit valamilyen speciális célból (pl. POS kiszolgálása) alakítanak ki.
DES - Data Encryption Standard: Szimmetrikus kulcsú titkosítási eljárás, blokk-rejtjelező, 64 bites blokkokat használ és 56 bites kulcso (64 bites blokkos rejtjelezés, vagyis a nyílt szöveg egy 64 bit méretű blokkjához rendel egy ugyanekkora rejtjeles blokkott). A DES a legelterjedtebb szimmetrikus rejtjelező, az USA-ban készült kormányzati felhasználásra. Az algoritmust 1977-ben hozták nyilvánosságra. Bár a DES kifejlesztése óta több mint 20 év telt el, ma is élő, még engedélyezett szabvány, széles körben használják a polgári élet minden területén, jóllehet a DES elérte életciklusának végét. A DES manapság nem nyújt megfelelő biztonságot, számos támadási mód létezik a DES ellen. A szabványok betartása miatt több helyen kötelező a DES implementálása, ám általában valamely korszerűbb rejtjelezést preferálnak ezek a programok is. A kissé idejétmúlt algoritmus felváltására már több alternatíva is van: a háromszor egymás után alkalmazott DES, vagy más alternatív algoritmusok (AES, IDEA, CAST, BLOWFISH). A DES kiterjesztése a 3DES, mely jóval nagyobb biztonsági szintet szolgáltat. **DES cryptosystem:** A Data Encryption Standard követelményeit teljesítő titkosító rendszer.
DES - Data Encryption Standard – Az USA 56 bites adattikosítási szabványa 1977-től.
DES3,3DES (Triple DES): Három DES titkosítás alkalmazása ugyanazon blokkon, legalább két különböző kulcs segítségével. Ennek következtében a kulcstér mérete és a kódolás minősége jelentősen javul. Középen találkozásos támadás során 2^112-re csökkenhet a DES3 erőssége az eredeti 2^168-as erősségről, de még így is biztonságosnak mondható.
DFS - Distributed File Service: Osztott file-szolgáltatás.
Digital Encryption - Digitális titkosítás: Az elektronikus dokumentumok biztonságát szolgáló elektronikus kódolási protokoll.
Digital signature: (digitális/elektronikus aláírás) Az üzeneteknek a nyilvános kulcsolási eljárás keretében történő aláírása, a küldő személyazonosságának elektronikus ezközzel történő igazolása. Egy üzenet vagy egy tranzakció hitelesítésére szolgáló üzenet, vagy tranzakciót küldő fél által használt rendszer. A digitális aláírást titkosító algoritmussal és az üzenetet küldő azonosítására szolgáló titkosító kulccsal generálják. Személyek és/vagy digitális adatok hitelesítésére alkalmas. Két részből áll: a személyhez kötött aláírást generáló részből, s az ellenőrzést bárki számára lehetővé tevő részből. Nyilvános kulcsú rendszer
Digitális Városháza (DV): Az Intelligens Város alapja. Egy belső hálózaton lévő web-oldal,, amit Internetről is el lehet érni. Az összes kapcsolódó megjelenik, megformálják a DV képet.
Digitising: (digitalizálás) Nem szöveges adat átalakítása digitális formára, különösen grafika-, ill. képfeldolgozásnál.
Disintermediation: (közvetítő kiiktatása) Folyamat, amikor a közvetítőt kiiktatják a tranzakcióból, és így a két elsődleges fél közvetlenül tud együttműködni.
Distributed data processing: (osztott adatfeldolgozás) Adatfeldolgozás hálózatba kapcsolt számítógépekkel, melyek megosztják a feladatokat egymás között.
DNS - Domain Name Service: Az Interneten a felhasználók számára értelmes neveket használnak gépek, szolgáltatások azonosítására, ezt a DNS rendszer segítségével alakítják át az egyértelmű IP azonosítókká (számokká). (Domain Name System, Domain Name Service, Domain Name Server: Az Internet-címek rendszere és a címek szerinti Internet-forgalmat biztosító szerverek szolgáltatásai.)
Domain name (Domain név) – Az interneten a Hostok címét jelölő, alfanumerikus formájú címzés. Ez az a cím, amit legtöbbször a www. karaktersorozat után írunk a böngésző címsávjába. (pl. www.mrsz.hu, ad.telnet.hu) ld. még: URL, Top Level Domain Name, Domain Name System
DoS - Denial of Service: Támadási cél, mely nem adatok megszerzését vagy megváltoztatását célozza meg, hanem számítógépek, hálózat vagy szolgáltatás használhatóságát próbálja rontani (a szolgáltatás megálljon, tönkremenjen, lefagyjon). Ide tartozik a számítógép elérhetetlenné tétele, a

valódi bejelentkezések ellehetetlenítése stb.
DRAM: dynamic random access memory: (dinamikus RAM), aminek minden memória ciklusban frissítenie kell a tartalmát.
DSA: Digital Signature Algorithm: digitális aláírás algoritmus, az USA állami szabványa.
DSB - Digital Sound Broadcasting – Digitális, műholdas rádióműsor sugárzás.
DSS: Digital Signature Systems: Távoli hitelesítésre használt aszimmetrikus titkosító, visszafejtő rendszer.
DSS - Digital Satellite System – Digitális műholdas rendszer.
DTE - Data Terminal Equipment: Adatvég-berendezés, pl. számítógép, terminál.
DVD - Digital Variable Disc: 1996-ban szab-ványosított igen nagy kapacitású (3-7 GB) optikai multimédia adattároló lemez, a CD-hez hasonlóan csak olvasható, többször írható változatai vannak.

E

eavesdropping: (lehallgatás) Az adattovábbítás nem engedélyezett lehallgatása. (hacker)
e-business: Az üzleti folyamat átalakítása a web-technológia és a meglévő informatikai rendszerek felhasználásával.
EBCDIC - Extended Binary Coded Decimal Interchange Code – Az IBM 8 bites adatkódja.
E-cash: Elektronikus pénz. Hitelesített érték, amit elektronikusan tárolt kód képvisel.
E-commerce Az e-business része, különböző üzletfelek, közigazgatási intézmények, végfelhasználókközött szervezett kereskedelem. Az elektronikus kereskedelemben jöl elkülöníthető részei: B2A, B2B, B2C, C2A, C2C.
EDI (Electronic Data Interchange): Elektronikus adatcsere: az okiratok papírmentes biztonságos cseréje.
EDIFACT: EDI for Administration, Commerce and Trade: elektronikus adatcsere az igazgatásban, és a kereskedelemben. Az Egyesült Nemzetek által kifejlesztett EDI szabvány, ami kombinálja az UN/GTDI és ANSI X12-t.
EEI - External Enviroment Interface: Az ember-gép kapcsolatot biztosító felület.
EEPROM: Electronically Erasable Programmable Read-Only Memory: elektronikusan törölhető, programozható ROM, ami sokszor újrafelhasználható, pl. az újratölthető elektronikus pénztárcákban. (nem úgy, mint az EPROM)
EFT: electronic funds transfer
EFTPOS: electronic funds transfer at point of sale
Electronic commerce: (elektronikus kereskedelem) Tranzakciók, amik elektronikus hálózaton történnek, ahol a kereskedő és a vásárló nem ugyanazon a fizikai helyen van. Pl.: kártyás tranzakciók az interneten keresztül.
Electronic data interchange: (EDI) Strukturált elektronikus adatcsere, az adatokat átalakítják a megfelelő formátumra a felek közötti továbbításhoz.
Electronic funds transfer at point of sale: (EFTPOS) Az árukért és szolgáltatásokért való fizetés technológiája és gyakorlata a vásárlás helyéről indított elektronikus pénzátutalással.
Electronic funds transfer: (elektronikus pénzátutalás) Számítástechnikai rendszerek funkcióiban megtestesült fizetési eszközökkel végzett fizetés technológiája és gyakorlata.
Electronic imaging: Digitalizált képek készítése optikaielektronikai eszközökkel, közvetlen fényképészeti rögzítés nélkül.
Electronic mail (e-mail): Elektronikus levelezés. Üzenetek elektronikus cseréje helyi és távoli számítógépek, végberendezések között, a helyi és a globális informatikai infrastruktúra segítségével. Az elektronikus levélhez csatolva dokumentumok, hang- és képfile-ok is lehetnek.
Electronic number plate: (elektronikus rendszámtábla) Egy eszköz, ami elektronikus jelet, többek között járműazonosító információt továbbít, és lehetővé teszi autópályadíj fizetését megállás nélkül.

Electronic payment terminal: Fizetési eszközt elfogadó terminál, amely elektronikus pénzátutalást végez.
Electronic point of sale: EPOS (elektronikus eladási pont) Az eladás helye, ami fel van szerelve elektronikus berendezéssel árazáshoz és a tranzakciók rögzítésére, de nem feltétlenül van elektronikus pénzátutalási funkciója.
Electronic purse/e-purse: (EP) (elektronikus pénztárca) Feltölthető integrált áramkörös kártya kis összegű vásárlásokhoz, pl.: VisaCash, Mondex és Proton
Electronic wallet: (elektronikus pénztárca) Egy szuperintelligens kártya, vagy zseb méretű intelligens kártya író/olvasó, ami összetett pénzügyi tranzakciók bevitelét teszi lehetővé, általában billentyűzeten keresztül.
EMMS - Electronic Mail and Messaging Systems – Elektronikus levelező és üzenetkezelő rendszer.
Encryption: (titkosítás) Információ átalakítása egy kulccsal, annak érdekében, hogy az értelmezhetetlen legyen illetéktelenek számára. A felhatalmazott címzett rendelkezik a kulccsal, amivel visszafejti az eredeti szöveget az ellentétes folyamattal (decryption).
EPROM: Electronically Programmable Read Only Memory. (Elektronikusan programozható csak olvasható memória) Eldobható kártyáknál, pl. telefonkártyáknál használják. (lásd még PROM)
ESP - Enhanced Service Provider: Értéknövelt szolgáltató, Internet-tartalom szolgáltató, lásd *ISP*.
Expert System - Szakértői rendszer: Az emberi szakértők problémamegoldását és analizáló képességeit szimuláló információs rendszer. A szakértői rendszerek hasznosak a rutinszerű, ismétlődő problémák kezelésében az emberi erőforrások teher-mentesítésére.
Exploit: a programok hibáira írt alkalmazás, célja a behatolás, vagy a károkozás.
extranet: Intranetes kapcsolat külső szervezetekkel, pl. szállítókkal.
Extranet: Kiterjesztett belső hálózat. A szervezerten belüli felhasználók kommunikációja külső felhasználók,általában fogyasztók vagy beszállítók csoportjával.

F

FAQ - Frequently Asked Question – GYIK, gyakran ismételt kérdés.
FCC - Federal Communications Comission – Az USA-ban a hazai Hírközlési Főfelügyelet megfelelője.
Feltörés (code breaking, attack): Az az eljárás, amikor egy rejtjelezett üzenetből a kulcs ismerete nélkül megfejtik az eredeti szöveget, vagy ami ezzel egyenértékű, a kódoláshoz használt kulcsot. Elképzelhető az is, hogy a támadó olyan alternatív algoritmust készít, amely a kulcs nélkül is képes a visszafejtésre. Ha a kódoláshoz használt kulcsot megtalálja a támadó és így a további üzeneteket gond nélkül olvasni tudja, akkor teljesen feltörtnek tekintjük a kommunikációt.
Fibre optic cables: (száloptikai kábel) Optikai üvegből készült szálakból összetevődő átviteli közeg, ami folytonos, megszakítás nélküli fényt továbbít, amin a digitális jelek közel fénysebességgel haladnak.
Fingerprint reader: (ujjlenyomat olvasó) Egy eszköz, ami digitalizált képpé alakítja az emberi ujjlenyomatot biometriai azonosítás céljából.
Firewall: (tűzfal) A vállalat számítógépes hálózatába történő elektronikus behatolás elleni védekezési módszer.
Fizikai biztonság (physical security): Fizikai akadályok és szabályzó eljárások alkalmazása, mint a megelőző intézkedések az erőforrások és az érzékeny információk fenyegetettsége ellen. Ahhoz, hogy egy csatorna biztonságos (secure) és ne csak biztosított (secured) legyen, szükség van fizikai védelemre is.
Flash: Egy igen népszerű program a Macromedia-tól. Segítségével a webfejlesztők importálhatnak különböző grafikus eszközöket, képeket, és különböző animációkat, különleges effekteket, hanghatásokat készítsenek. A tartalom ezután fileként mentődik .SWF kiterjesztéssel.
Frequency modulation: (frekvencia moduláció) Jelek rögzítése az alternatív áramirány

változtatásával. Gyakran használják megtévesztő módon a two frequency recording kifejezést.
Front-end processor: Számítógép, amely egy általában nagyobb számítógép kommunikációját kezeli.
FSS - Fixed Satellite Service – Főként a professzionális távközlési szolgáltatások műholdjai
FTP - File Transfer Protocol: Az Internet egyik igen régi, fájlok átvitelére szolgáló authentikált protokollja, TCP csatornán keresztül. A bejelentkezés során a jelszavak kódolás nélkül mennek át a hálózaton. Javasolt helyette más, például SSL-es FTP, SCP használata.

G

gateway: Eszköz, mely összekapcsol két különböző számítógépes hálózatot, és belső hálózati protokoll átalakítást végez.
GB - Gigabyte (109 byte).
Generalised Advanced Urban Debiting Innovations project (GAUDI): Az Európai Közösség által támogatott projekt, ami öt nagy európai városban működik, és intelligens kártya projekteket is magába foglal.
gigabyte: Egy milliárd byte.
GEO- Geostacionary Earth Orbit – 35 786 km magasságú műholdpálya, a keringési idő 23,934 óra, megegyezik a Föld forgásidejével.
Global System for Mobile communications (GSM): Mobil kommunikáció globális rendszere. (eredeti elnevezése Groupe System Mobile) Világszerte bevezetett digitális mobiltelefon hálózat, ami nagyobb kapacitással és jobb átviteli minőséggel rendelkezik, mint az analóg hálózatok.
GPS: Global Positioning System. (globális pozícionáló rendszer) Az USA állama által bevezetett műholdas navigációs rendszer. (GSM: Global System for Mobile Communications)
GSM - Global System for Mobile Communications: A pán-európai digitális mobil kommunikációs szabvány, (eredetileg a témával foglalkozó Groupe Special Mobiles 1987, francia csoport neve), 1991-ben kezdték nyilvános használatát. Digitális, celluláris mobil rádió a 900 MHz-es sávra. A magasabb frekvenciájú DEC 1800 a GSM változata.
GUI: Graphical User Interface. Grafikus felhasználói felület, például a Windows.

H

hacker: Egy személy, aki megpróbál engedély nélkül, nem rosszindulatúan számítógépes rendszereket elérni/feltörni, tehát olyan számítógépes szakértő, aki rendszereket tör fel vagy megbízásból vagy ’hobbiból’, de abban nem tesz kárt. (lásd még cracker) Hacker, Cracker pontos jelentésének definíciói változatosak. A hacker jelent jószándékú „ráérő' típusú programozót, aki saját örömére átír programokat, hogy azok jobbak legyenek. A hacker másik definíciója a cracker szóval mosódik össze, ekkor számítógépes bűnözőről beszélünk, aki számítógépbe, vagy számítógépes rendszerekbe jut be, azt illegálisan használja. Egyes hackerek nem is igazán értik amit csinálnak, ezért további kategória az überhacker, aki a többi hackernél okosabb, ő ismeri fel az alapvető biztonsági hibákat. A hackerek nem szokták magunkat számítógépes bűnözőként azonosítani, még ha pusztítás is a szándékuk. Hackerek nélkül az Internet kevésbé lenne biztonságos.
Hash függvény: Olyan transzformáció, amely egy tetszőleges hosszú szöveg digitális 'ujjlenyomatát' készíti el. Az 'ujjlenyomat' fix hosszú bitsorozat amely jellemző az adott szövegre abban az értelemben, hogy más szöveghez szinte biztosan más hash érték tartozik, illetve adott ujjlenyomathoz gyakorlatilag lehetetlen olyan szöveget találni amelynek ez a képe. Nevezik message digestnek is, a Digitális aláírás protokoll alkotórésze
Hírközlés - Általános fogalom, mely magában foglalja a hírek és információk átvitelének,

tárolásának és feldolgozásának számos területét, jelesül a távközlési szolgáltatásokat (beleértve a közcélú és külön célú vezetékes és mobiltelefoniát és adatátvitelt), a rádió és televízió műsorszórást, műsorelosztást és műsorszétosztást, valamint a postai szolgáltatásokat. A hírközlő rendsze-rek alaptulajdonsága, hogy az átvitt információ tartalmától függetlenül működnek, korunkban tapasztalható forradalmi fejlődésük abban is megnyilvánul, hogy átlátszó és tartalomfüggetlen átviteli szolgáltatásokat biztosítanak. Mindezek a modern információs társadalom infrastrukturális alapelemei, melyek nélkül a nemzeti informatikai fejlesztési stratégia nem valósítható meg.
Távközlés: minden folyamat, amely megfelelő formájú információ (nyomtatott másolat, álló vagy mozgó kép, látható vagy hallható jelek stb.) továbbítását szolgálja az adótól egy vagy több vevő felé, bármilyen elektromágneses rendszer (vezetékes elektronikus átvitel, rádió, opti-kai átvitel, csőtápvonal stb.) útján. Ide tartozik a távíró, telefon, videotelefon, adatátvitel stb.
Hit: ezzel a számmal a webszerverre történő kapcsolatok számát határozzák meg. Minden felszólítás egy új adatfájl letöltésére egy HIT-et eredményez. Minden Weboldal különböző számú fájlt (háttérkép, háttérzene, az oldalon található képek, alkalmazások stb.) tartalmaz. A Website-ok megtekintésének alapegysége egy oldal letöltése (egy Page Impression), tehát a találatok száma nem ad az oldalak látogatottságára, vagy a Page Impressionök számára vonatkoztatható információt. Azaz, ha feltételezzük, hogy egy Website egyetlen oldalát egyszer egyvalaki megnézi, akkor ha az adott oldalon sok kép van, akkor sok találat keletkezik, ha nincs rajta kép, akkor csak egy találat keletkezik, pedig az oldalt összesen csak egyszer nézték meg.
Hitelesítés: A hitelesítés módszer arra, hogy az üzenet vevője biztos lehessen a küldő személyében és/vagy a kapott üzenet integritásában.
hologram: Sík optikai kép, ami háromdimenziósnak látszik. Gyártásához bonyolult, drága felszerelés szükséges, ami koherens fény használatával készíti a képeket.
home banking: Lakossági bankműveletek, amiket az ügyfelek saját otthonukból elektronikus fizetési terminálokon keresztül bonyolíthatnak le.
Homepage (Kezdőoldal): A Website bevezető oldala és általában tartalomjegyzéke, ahonnan a Website szinte bármelyik részére eljuthatunk. A honlap általában az az oldal, ami egy Domain név beírásakor megjelenik.
Host: Olyan számítógép, amelyik az Internetre csatlakozik, függetlenül attól, hogy rajta keresztül hány felhasználó használja a szolgáltatást. Ha ez a számítógép egy szerver, akkor a hozzá kapcsolódó többi számítógépnek erőforrásokat biztosít.
host-to-host authorisation: Egy olyan módszer, ahol az autorizáció során a kereskedő számítógépe közvetlenül kapcsolatba lép a szolgáltató hosttal.
HSCSD (High Speed Circuit Switched Data): mobiltelefonokban használatos, az adatátvitel gyorsaságát növeli meg
HTTP: (Hyper Text Transfer Protokoll) Web szerverek és előfizetők közötti adatátviteli protokoll.
HUB: Egy olyan oldal az Interneten, vagy belső hálózatokon, amelyen minden megtalálható, ami egy témában rajta lehet: egy gondolat köré csoportosít minden információt és ami abban a témában működik bemutatja
hybrid card: Kártyák, melyek gyártásakor egynél több technológiát ötvöznek. Pl.: chipet és mágnescsíkot is tartalmazó kártya.
hybrid tűzfal: egy proxy és egy alkalmazás szűrő ötvözete
Hyperlink (Link): A HTTP szabvány nyújtotta lehetőségeket kihasználó utalás, ami egy máshol található információra mutat, segítségével a hivatkozott információ megtekinthető.
Hypermail - Program, a UNIX postafiók üzeneteiből (pl. egy hírcsoport levelezése) kereszthivatkozásokkal ellátott dokumentu-mokat állít elő és tesz hozzáférhetővé.
Hypertext - Nemlineáris olvasás, írás amelyben a felhasználó a megfelelő információt az elektronikusan meghatározott mutatók segítségével bármilyen sorrendben megnézheti. A hipertext alkalmazása a számítógépen elérhetővé teszi a helyi vagy a hálózat távoli gépén elektronikusan tárolt dokumentumot.

I

IDEA: International Data Encryption Algorithm. Nyolc input bájtot nyolc output bájtra képező blokkos rejtjelező algoritmus. Kulcsmérete 128 bit. Svájcban fejlesztették ki 1990 és 1992 között. Kifejezetten adatátvitelhez tervezték, beleértve a digitalizált hang/kép valós idejű kódolását is. A PGP régebbi verziói is használták. Szabadalmi bejegyzése van, és így (üzleti) felhasználásához licenszdíjat kell fizetni. Egy ideig a DES ellenfelének tűnt, de ma már nem igazán preferálják, kissé háttérbe szorult.
IDL - Interface Definition Language.
IDS - Intrusion Detection System: Figyelő, analizáló és cselekvő rendszer vagy eszköz, mellyel rosszindulatú betörő vagy annak valamilyen cselekedete leleplezhető.
IETF - Internet Engineering Task Force: Az Internet működtetésével és fejlesztésével foglalkozó szervezet, melynek alszervezetei, bizottságai végzik a legfontosabb és legalapvetőbb Internetes „szabványok" elfogadását.
Információ: Olyan jelentéssel bíró szimbólumok összessége, amelyek adatokat tartalmaznak és olyan új ismereteket szolgáltatnak az értelmező számára, hogy ezáltal annak valamilyen bizonytalanságát megszüntetik és célirányos cselekvését kiváltják.
Információs rendszer - Hálózat: többszörös működtetési szintű, de egy (a tervezési, ellenőrzési és mérési folyamatokra vonatkozó) menedzsmentorientált rendszer. A hálózat biztosítja az információs rendszerhez tartozó különböző adatbázisok adatainak elérését és szintetizálását a szervezet működése számára fontos információkká.
Információtechnológia - Röviden **IT**, az adatfeldolgozás és a távközlés együttes alkalmazásának ágazata: magába foglalja a számítógépet és az irodaautomatizálást, a vonatkozó szoftvereket, a távközlési lehetőségeket, mindazt, amely az információ gyűjtését, feldolgozását, tárolását, elosztását és megjelenítését lehetővé teszi, azaz az elektronikus alkatrész- és kommunikációs ipart, de ide értjük a vonatkozó termékek fejlesztését, gyártását, illetve szolgáltatások nyújtását és a marketinget is. Nem tartozik ide a szórakoztató elektronika, a termelés-automatizálás és a katonai alkalmazások.
Informatika - Az információk gépi feldolgozásának és közvetítésének tudománya – az információs és kommunikációs technikákkal és azok szakágazatokban történő alkal-mazásával foglalkozik. Lásd még *Információtechnológia*, *Telematika.*
Information & Referral (I&R) Services - Információs és dokumentációs szolgáltatások – Integrált szolgáltatások, amely az egyéneket, szervezeteket, családokat és közösségeket segítik a problémák és feladatok megoldásában a megfelelő források megtalálásában és használatában. Lehetőség van az erőforrás gazdálkodásra is.
Integrated circuit: (integrált áramkör) Félvezető anyagon létrehozott elektronikus áramkör.
Interactive Electronic Services - Interaktív elektronikus szolgáltatások – Olyan számítógépes, terminálos, telefonos vagy TV-s szolgáltatások, amelyek információ cserét, kommunikációt, tranzakciókat és a kikapcsolódás-szórakozás kategóriájába eső tevékenységet jelentenek. A szolgáltatások otthonról, nyilvános helyekről vagy munkahelyről is igénybe vehetők, például az audiotext, videotext, telebank, BBS.
Interbank transfer: Bankközi átutalás.
Interface - Interfész csatlakozó, illesztő felület, amely lehet egy pont, konvertáló hardver és szoftver, eszköz, pl. az ember-gép kapcsolatban a grafikus képernyőfelület, a GUI.
intermediate network facility: (közvetítő hálózati szolgáltatás) Számítástechnikai és telekommunikációs berendezések rendszere, ami támogatja a tranzakció átvitelt kialakított rendszer résztvevői között.
International Standards Organisation (ISO): Ipari szabványok kialakítására, és ezeknek a nemzeti szabványügyi testületekhez való terjesztésére megalakított svájci székhelyű központi testület.
Internet: A Federal Networking Council 1995-ös definíciója: Az “Internet” globális információs

rendszer, amely 1. az Internet Protokoll (IP), illetve megfelelő kiterjesztései, változatai alapján képzett globális címteret logikailag összekapcsolja; 2. lehetővé teszi a kommunikációt a TCP/IP, illetve megfelelő kiterjesztései, változatai és/vagy más IP kompatibilis protokollok alapján, és 3. nyilvános vagy privát használatát vagy elérését biztosítja a kommunikációs vagy itt leírt vonatkozó infrastrukturális rétegekre telepített magas szintű szolgáltatásoknak. Más meghatározás: az Internet a hálózatok globális hálózata, melyet a nemzeti és akadémiai-kormányzati hálózatok összekapcsolásával azonos technológia alkalmazásával hoztak létre. Magába foglalja a távközlési vonalakat, kapcsológépeket, számítógépeket, hálózati protokollokat, és az együttműködést és információátvitelt biztosító szolgáltatásokat. A kilencvenes évek Internetje az egész világra kiterjedő informatikai infrastruktúra prototípusának tekinthető. Világméretű, kisebb helyi hálózatokat egymással összekötő számítástechnikai rendszer. Közös konvenciók, egyezmények és eszközök következtében egy homogén hálózatnak látjuk, holott az így összekötött gépek nagyon sok különböző hardvert, illetve szoftvert használnak.
Interoperability: Egy rendszernek az a képessége, hogy képes különböző rendszerekben kezdeményezett tranzakciókat kezelni
Interstitial – Egy olyan Pop-up ablak, amely korlátozott időtartamban jelenik meg. Az időtartam (néhány másodperc) lejártával az ablak automatikusan becsukódik.
“in-the-wild”: számítógépavírusok legrettegettebb csoportja
Intranet: Az internet mellett megjelent fogalom. Az intranet TCP/IP-, illetve web technológiájú hálózat, a vállalton belüli kommunikációeszköze. Vagy önálló vagy csak tűzfalon (firewall) keresztül kapcsolódik az internethez.
IP - Internet Protocol: Az Internet alapját jelentő átviteli protokoll, a TCP/IP stack alsó rétegét jelenti, így gyakorlatilag minden Internetes adatforgalom ezen alapul. Jelenleg a IPv4 az általánosan elterjedt változata.
IP Address (Internet Protocol Address, IP cím) – A World Wide Web-csomópontok számmal megadott címe, amelyet az ún. Nameserver azonosít az URL címmel. Ebből következik, hogy a szövegesen megadott Web-cím megváltozhat, de ha erről a Nameserver tudomást szerez, akkor a régi Web-címre érkező kéréseket át tudja irányítani az új címre, mivel az IP cím nem változik. (formája pl.: 256.546.247.333)
IP cím: Az Internet hálózatában a gépek egyértelmű azonosítását lehetővé tevő szám.
IPSEC: Az IPSEC, azaz az IP Security Protocol egy olyan biztonsági protokoll, melyet az IETF, az Internet Engineering Task Force fogadott el az IP szintű biztonság növelése érdekében. Munkámban külön fejezetben ismertetem alapjait.
IPv4: Általánosan elterjedt IP verzió, 32 bites címeket tartalmaz. Az IPSEC biztonsági szolgáltatásai IPv4 alatt is megvalósíthatóak.
IPv6: Következő generációs Internet protokoll. Számos kiegészítést tartalmaz, a gépek azonosítását egy hierarchikus 128 bites számmező végzi. Biztonsági szolgáltatásainak egyike lesz az IPSEC.
IRD - Integrated Receiver Decoder, lásd *set top-box*.
ISDN: Integrated Services Digital Network (koordinált szolgáltatású digitális hálózat) A közszolgálati telefonos hálózat közvetlen alternatívája. Lehetővé teszi digitalizált adatok nagy sebességű továbbítását.
ISP - Internet Service Provider: Internet-szolgáltató. Vö. *ESP*, *KIP*.
ITU - International Telecommunication Union – Az ENSZ speciális szervezete 1992-től. Tevékenységét tekintve a genfi CCITT és CCIR feladatait is átvette. Szabványosítási, ITU-T és ITU-R szekciók működnek. Az ITU a világ távközlés fejlesztését, hatékony használatát és harmonizációját segíti.

J

Java: Egy olyan programozási nyelv, mellyel különböző géptípusokon egyformán futtatható szoftverek írhatók. Igazából a World Wide Web terjedésével lett népszerű, mint az azt kiegészítő

alkalmazások gépfüggetlen programnyelve. Az új Böngészők már "értik" a Java nyelvet, vagy annak egyszerűsített, JavaScript nevű változatát.
Java: A Sun Microsystems által kifejlesztett platform független programozási nyelv, ami a C++-on alapszik és az intelligens kártyákat a futó szoftverek szabványos platformjára fordítja. A Java nagyon elterjedt az Interneten.
Javascript – A Java programnyelv egyszerűsített változata.

K

KBS: knowledge-based system. (tudásalapú rendszer)
Kernel: Az operációs rendszerek magja. Linux esetén a kernel végzi a hálózati kapcsolatokkal kapcsolatos alacsonyabb rétegű szolgáltatásokat, bár rövidesen kernel szintű http kiszolgálás is implementálva lesz. A kernel folyamatosan fejlődik. A linux kernelébe a tűzfalaknál szükséges szűrő lehetőségek is implementálva vannak. A kernel moduláris és kiegészíthető a linux operációs rendszerben.
key management: (kulcs kezelés) A kulcs biztonságos előállítása, hozzárendelése személyekhez, a kulcs terjesztése és cseréje a titkosító rendszerben.
key: (kulcs) A titkosítás és visszafejtés folyamata során a bizalmas információ átalakításához használt érték. A visszafejtés könnyű a kulcs birtokában, nélküle viszont nagyon nehéz. A biztonság a kulcs titokban tartásán alapul.
kilobit (kb): 1024 bit
kilobyte (kB): Pontosan 1024 byte. A számítógép memóriakapacitásának, vagy egy fájl méretének mértékegysége. A rövidítése K. (pl. 254K)
KIOSK - Információs kioszk: Nyilvános, interaktív elektronikus terminál, amely a közhasznú információkhoz való hozzá-férést segíti. Kioszk lehetne egy személyzettel üzemeltett ügyfélszolgálati pont is, de ma már inkább a billentyűs, érintős vezérlésű képernyővel ellátott, hálózatra kapcsolt berendezéseket jelenti, ahol a polgárok az őket érdeklő információkat megszerezhetik vagy üzeneteket, tranz-akciókat továbbíthatnak harmadik személy közreműködése nélkül.
Kriptoanalízis: a titkosított szöveg dekodolása az eredeti szöveg, vagy a kulcs ismerete nélkül. A Kriptográfia ellentétpárja, adatvédelmi rendszerek támadásával, feltörésével foglalkozó tudomány.
Kriptográfia: Az információ algoritmikus módszerekkel történő védelmének tudománya.
Kriptológia: Az algoritmikus információvédelem és ezen módszerek támadásának tudománya, a Kriptográfia és a Kriptoanalízis összessége.
Kulcs: A rejtjelző rendszer rejtjelzési módszerek halmaza. A kulcs ezen módszerek címkéje, vagyis a kulcs által választódik ki az éppen alkalmazott rejtjelzési transzformáció. A kulcs az az információ, ami nélkül nem lehet a titkosított üzenet tartalmához hozzáférni. Ha mindkét félnek ugyanarra a kulcsra van szüksége, akkor szimmetrikus kulcsú titkosításról beszélünk. Ha a kódoláshoz más kulcs szükséges, mint a dekódoláshoz, akkor aszimmetrikus- vagy nyilvános kulcsú titkosításról beszélünk. Jó algoritmus esetén a kulcs által biztosított védelem exponenciálisan arányos a kulcs (bitekben mért) hosszával.

L

LAN (Local Area Network): Helyi hálózat, viszonylag gyors adatátvitellel, kevés géppel. Adat feldolgozó hálózat, mely egy csoport azonos helyen lévő - felhasználót szolgál ki, és nem használ nyilvános telekommunikációs hálózatokat.
language: (nyelv) Szabályok és szimbólumok rendszere. pl.: Basic, Fortran.
Lead: A látogatók által körkérdésekre, vagy nyereményjátékok alkalmával megadott elérési címek, illetve egyéb személyes adatok. Az egy személy által egy alkalommal megadott adatok összesen

egy leadnek számítanak.
Lehallgatás (wiretrapping): Valós idejű gyűjtése a közvetítet adatoknak, mint például: tárcsázott számjegyek, beszélgetések vagy egy vevőkészülékre küldött adatoknak a lehallgatása, tárolása.

M

MAC - Message Authentication Code (üzenet hitelesítő kód): Olyan Kulcstól függő kontrollösszeg, amely a vevőoldalon az adatok véletlen és szándékos módosítását egyaránt képes detektálni.
Magnetic shielding: (mágneses árnyékolás) Elektronikus alkatrészek bevonása védő burokkal az elektromágneses zavarok és a kisugárzás megelőzésére.
MAN (Metropolitan Area Network):Mint neve is mutatja a nagyvárosok térségében üzemelő hálózat, fejlett technika, sok-gépes hálózat.
management information system (MIS): vezetői információs rendszer
Man-in-the-middle típusú támadás: Ha egy hálózati forgalmat egy közbenső személy meg tud csapolni, akkor mód van arra, hogy ez a közbenső személy a hálózati forgalom mindkét résztvevője felé az eredeti partnernek adja ki magát. Nem megfelelő protokoll esetén ekkor egy egyszerű kódolt csatorna is dekódolhatóvá válhat.
masked ROM: ROM, amibe az adatot a gyártás során beépítették, és azt utólag nem lehet törölni és újra programozni. (lásd még PROM, EPROM, EEPROM)
Masquerade,NAT,Native Address Translation: ezeket a fogalmakat azokra a megoldásokra alkalmazzák, ahol egy hálózati berendezés valamilyen okból egy hálózat vagy egy gép IP címét átalakítja. Ez az átalakítás úgy is történhet, hogy az Internet felé a kéréseket saját nevében továbbítja (masquerading), vagy pl. úgy, hogy valamely szabály alapján alakítja át az IP tartományokat az Internet irányában. A megoldás sokrétűen felhasználható a kevés kioszthető IP szám következtében fellépő problémákra, vagy a biztonságosság növelésére (anonimizálás).
megabyte (MB): Pontosan 1.048.576 byte.
Megszemélyesítés (mimicking): Olyan rendszer hozzáférési törekvés, amelyben a jogtalan felhasználó úgy tesz, mintha ő egy jogos volna. (Szinonim kifejezések: megszemélyesítés, álcázás, utánzás, pózolás) Általában aktív támadást és beékelődést jelent a kommunikáló felek közé.
message authentication code (MAC): (üzenet hitelesítő kód) A fizetési rendszerben használt kód, amivel az üzenet eredetiségét igazolják.
microprocessor: Az a részegység, amelyik a számítógép központi egységének szerepét tölti be. A mikroprocesszor az elektronika miniatürizálási technikájának és a számítástechnika fejlődésének eredménye, kis méretben, alacsony költséggel programozható intelligenciát nyújt.
Microsite – Néhány oldalból álló Website, mely nem tartalmazza az összes információt, csak azokat, amik relevánsak. Általában promóciókhoz, piackutatásokhoz használják. Elhelyezését tekintve lehet a vállalati ill. termék-Website, vagy egy nagyobb Website speciális része.
MIME - Multipurpose Internet Mail Extensions – Internet e-mail.
MIS - Management Information System.
MLLN - Maneged Leased Line Network – Digitális béreltvonalas szolgáltatás.
modem: Elterjedten a szabványos, kapcsolt telfonvonalon a számítógépes kommunikációt lehetővé tevő berendezés. A “modulator/demodulator” szavak összevonása. A számítógépről jövő digitális információt átalakítja analóg jelekre a telefonvezetéken történő adattovábbításhoz, azután a fogadó modem visszakonvertálja azt digitális információvá.
Mondex: Elektronikus pénztárca rendszer. Az 1996-ban alakult, világszerte 17 szervezetet magába foglaló Mondex International felügyeli a globális márkanevet és védjegyezést, technológiafejlesztést, nemzetközi működést, biztonságot, kockázat menedzsmentet és a Mondex licencek eladását olyan országokban, ahol a franchise-t még nem vették meg. 1996 novembere óta a MasterCard-nak 52%-os részesedése van a Mondex International-ban.
Monoalfabetikus titkosítás (monoalphabetic encrypting): Olyan rejtjelezési módszer, melynél

egy kódolatlan szimbólumot egyetlen kódolt szimbólumnak feleltetünk meg.
Moore törvénye (Moore's law): A számítási kapacitások, pontosabban a processzorok teljesítménynövekedésére vonatkozó állítás: a processzorok teljesítménye 18 hónap alatt megduplázódik. Többek, például Stan Williams (HP vezető tervező) szerint ez az ütem a közeljövőben lassulni fog, mert az egyre kisebb áramköri lapkákat eredményező szilícium alapú MOS-FET technológia már nincs messze a kvantum-mechanika által állított határoktól.
MPEG - Az ISO Motion Picture Experts Group digitális videotömörítési szabványa.
multimedia: Technológia, ami ötvözi a hangot, grafikát, képet és szöveges anyagokat, az információ egynél több formátumban, médiumon történő számítógépes terjesztése. Azaz a szöveg, grafika, animáció, video (egyszóval álló vagy mozgó kép) és hanginformációk közül legalább egy statikus és dinamikus egyidejű megjelenítése. Sokan minden számítógépes alkalmazást, ami hangot és/vagy videot tartalmaz, multimédiának neveznek.
Műszaki sebezhetőség (technical vulnerability): Egy hardver, szoftver vagy kommunikációs hiba, amely lehetőséget nyújt egy számítógépes rendszer potenciális kihasználásra vagy támadására a rendszeren kívül vagy belül. A hiba veszélyezteti a rendszer működőképességét és közvetve tulajdonosát, felhasználóját.

N

National Bureau of Standards (NBS): (Nemzeti Szabványügyi Testület) Az amerikai National Institute of Standards and Technology szervezet elődje.
National Institute of Standards and Technology: (Nemzeti Szabványügyi és Technológiai Testület) Az USA szabványügyi szervezete.
NCP: network control program
NETBIOS - Network Basic Input/Output System – A Microsoft és az IBM által létre-hozott személyi számítógépes de facto szabvány az OSI 5-ös viszony rétegre.
network architecture: (hálózati architektúra) Számítógép és kommunikációs rendszerek összessége, ami a köztük lévő kommunikációt és együttműködést támogatja.
network control programme (NCP): (hálózat irányító program) Egy program, ami egy számítógépes hálózatban irányítja az adatátvitelt.
network protokol: (hálózati protokoll) Egy közvetítő hálózati szolgáltatásban a hálózat által összekapcsolt elemek közötti kommunikációt irányító eljárások és szabályok összessége.
network: (hálózat) Számítástechnikai rendszerek összessége, amik kommunikációs kapcsolatokon keresztül működnek együtt, és kommunikálnak egymással.
neural network: (neurális hálózat) Intelligens, csalás megelőző öntanuló rendszer, ahol a szoftver tanul és módosítja a viselkedési modellt.
NII - National Information Infrastructure – Nemzeti Informatikai Infrastruktúra. Fejlesztésére a legtöbb országban stratégiát alakítanak ki. Az informatikai infrastruktúra összetett fogalom, tartalmazza: 1. az univerzális elérést biztosító egymással összekapcsolt és együttműködő távközlési hálózatokat; 2. számítógépeket, televíziót, faxkészülékeket, telefonokat minden informatikai eszközt; 3. az információs rendszerek adatbázisait és szolgáltatásait (pl. elektronikus könyvtár, elektronikus katalógus), és 4. az emberi tudást, a képzett polgárokat, akik fel tudják építeni, üzemeltetik és fenntartják az infrastruktúra elemeit egyenként és összességükben.
Nyílt: Az eredeti üzenetet nyiltnak, vagy nyílt információnak nevezzük.
Nyilvános: A nyilvános kulcsú rendszer alapgondolatát 1976-ban kulcsú rendszer találta ki W. Diffie és M. Hellman. Az addig egyeduralkodó szimmetrikus kulcsú rendszerek esetén az adó és vevő előre kulcsot cserél egy biztonságos, nem lehallgatható csatornán, s ilyenkor a rejtjelzés és megoldás ugyazzal a kulccsal történik. A nyilvános kulcsú rendszerben a rejtjelzéshez és a megoldáshoz szükséges kulcs nem azonos, a rejtjelző kulcsból a támadó nem tud a megoldó kulcsra következtetni. Ezért elég csak a megoldó kulcsot titokban tartani, a rejtjelzéshez szükséges kulcs

nyilvánosságra hozható, mint a telefonszámok a telefonkönyvben. Az első, ezen elv alapján működő rendszer az RSA volt.

O

OCR: optical character recognition (optikai karakter felismerés)
off-line: Papír alapon, vagy elektronikus terminálon végzett tranzakció, ahol a tranzakció során az elfogadói terminál és egy központi számítógép között semmilyen kapcsolat nincs.
OMR: optical memory reader
One-Stop Shopping - Egyetlen információs forráson biztosított teljes körű közszolgálati vagy magán célú szolgáltatások és termékek megszerzése. Mindez információs kioszk, személyi számítógép kábeltévé, telefon vagy más hálózati eszközzel bonyolítható, anélkül, hogy a szolgáltatást vagy terméket kereső különböző hivatalokba, irodákba, boltokba járna, és ott hasonló vagy éppen egymásnak ellentmondó elő-írásokkal küzdene, hogy igényeit kielégítsék.
one-time PROM:PROM, amire ha egyszer adatot helyeznek, az nem törölhető, és nem újraírható. (Lásd még EPROM, EEPROM)
on-line authorisation: (on-line engedélyezés) A tranzakció engedélyezésének az a típusa, amikor egy engedélyező központ végzi el azokat az ellenőrzéseket, amik a tranzakció engedélyezéséhez szükségesek.
on-line: Terminálon végrehajtott tranzakció, ahol a terminál állandó kapcsolatban van egy hálózattal, vagyis a kártyaszámlával.
on-line-áruház: többféle terméket kínál eladásra a neten keresztül.
on-line-áruház: többféle terméket kínál eladásra a neten keresztül.
optical fibre: (optikai szál) fibre optic cables
OSI - Open Systems Interconnection – Nyílt rendszerek összekapcsolása, ISO szabvány.

P

packet: csomag, az adatátvitelben használják
packet-switching network: (csomagkapcsolt hálózat) Kommunikációs rendszer, ahol az adatokat különálló csomagokra bontva továbbítják.
Page Impression (Page View, Oldalletöltés): ez a szám fejezi ki, hogy hány teljes oldalt töltöttek le. Egy teljesen letöltött oldal tehát egy Page Impression-t eredményez, függetlenül az oldalon szereplő adatfájlok számától. A Page Impression tehát egy Weboldal (általában egy képernyő-oldal, de gyakori, hogy az oldal "lefelé" görgethető) sikeres letöltődése esetén keletkezik. Az Weboldal bármilyen információt (képi, szöveges, dinamikus) tartalmazhat. A Page Impression akkor jön létre, ha a Weboldalon található minden elem teljes terjedelmében sikeresen letöltődött. A Magyar Internet Audit Tanács szabványa szerint a felhasználó által fogadott, a szerver által egyedi dokumentumként elküldött fájl, vagy fájlok kombinációja, amely a felhasználó egyedi kérésének eredményeként került elküldésre.
Password, jelszó: Jelszó, az adott felhasználó azonosítását lehetővé tevő jelhalmaz. A jelszavakat a mai rendszerek többsége nyílt szöveg formájában vagy kódolt változatban tárolja, a kódolt változat általában egyirányú függvénnyel titkosított, így nem visszafejthető. A kódolt jelszó nem védett a szótári próbálkozásoktól. A legelterjedtebb UNIX-os jelszórendszer DES algoritmust használ, maximum 56 bit hasznos információval, de a nyelvi sajátosságok miatt az átlagos információtartalom 30 bit körüli csak (vagy még kevesebb).
Patch: Javítás, hibajavítás, esetleg a fájlbeli különbségek kijegyzetelt változata.
payment system: (fizetési rendszer) általánosan egy fizetési eszközöket feldolgozó, a felek között keletkező adósságokat elszámoló rendszer. Pl.: Europay International, MasterCard International, Visa International. Ez a kifejezés ma gyakran használatos a pénzügyi intézmények által használt

számítógép rendszerek és szoftverek megnevezésére is.
PBX - Private Branche eXchange – Telefonalközpont.
PC - Personal Computer – Személyi számítógép.
PDA - Personal Digital Assistant – 160 grammtól 500 grammos "zseb"számológép, előjegyzési, naptár, telefonkönyv, esetleg modemes, faxos csatlakozás telefonvonalra, PC-re, több Mbyte memória.
personal identification number (PIN): (személy azonosító szám) A kártyabirtokosoknak kiosztott szám, amivel egyértelműen azonosíthatják magukat a vásárlás helyén. Ez a szám általában 4 számjegyű, és a kártyabirtokosnak meg kell azt jegyeznie.
PFM: Personal Service Manager, a családi költségvetés, és fizetések nyilvántartását támogató szoftver
PGP: 1991-ben Philip Zimmermann olyan programot írt, amely az RSA nyilvános kulcsú módszert az IDEA szimmetrikus kulcsú módszerrel kombinálva e-mail (és fájl) titkosítására teszi alkalmassá. Az újabb verziók már DSS/SHA – CAST algoritmusokat is használják. A program igen sok port és vitát kavart a kormányzati szinten, mert egyrészt az engedélyezett méretű kulcsokon túl a jóval hosszabb és biztonságosabb kulcsok használatát is lehetővé tette, másrészt nemzetközi elterjedése (az Interneten keresztül), megsértette az USA fegyverexport tilalmát.
PIC: Personal Identification Code. (személy azonosító kód) Négy, vagy hat számjegyű kód, ami hozzáférési lehetőséget nyújt elektronikus eszközökhöz a debit, vagy credit kártya használata során, és a kártya elvesztésekor biztonságot nyújt. (Lásd PIN)
piggybacking (tailgating): Számítógéphez való illetéktelen hozzáférés módszere, úgy hogy egy engedélyezett alkalmazott nyomait követik.
Plugin: A Böngésző alapszoftverét kiegészítő szoftvermodul. A modulok által kínált kényelmi funkciók nem szerves részei a Böngészőknek, ezért azokat külön kell letölteni a készítő Website-járól. Általában ingyenesek. A legelterjedtebb Plugin-ek a különböző képi, audio- és videoállományok megtekintését teszik lehetővé a Böngészőben.
point of sale terminal: (POS terminál) A kereskedőnél elhelyezett eszköz, ami a bank rendszeréhez telefonvonalon keresztül kapcsolódik, és eladáskor az adatok elektronikus formában kerülnek engedélyezésre, regisztrálásra, és továbbítására.
Polialfabetikus titkosítás (Polialphabetic encrypting): Olyan rejtjelezési módszer, melynél egy kódolatlan szimbólumot több különböző kódolt szimbólum reprezentál
Pop-up banner (Felbukkanó reklám): Hasonló a Felbukkanó ablak-hoz, azzal a különbséggel, hogy egy Banner bukkan fel hirtelen, amikor letöltjük a Website-ot.
Pop-up window (Febukkanó ablak): Egy Website letöltésekor automatikusan felbukkanó új ablak. Általában arról a Websiteról tartalmaz információkat, amelyet letöltöttünk. Ezek többnyire akciók, hirdetések.
POS: point-of-sales, a kereskedőknél elhelyezett kártyaleolvasó terminál
Private key: (személyes kulcs) Az aszimmetrikus titkosításnál az a kulcs, ami a nyilvános kulcs párja. Amit a publikus kulccsal titkosítanak az a hozzá tartozó privát kulccsal fejthető meg.
Programmable read-only memory: Csak olvasható memória, aminek a tartalma feltölthető a gyártás után a felhasználó által. (lásd még masked ROM) Néhány típus lehetővé teszi a tartalom törlését, és új adatok feltöltését, pl. EPROM (erasable PROM) és EEPROM (electronically erasable PROM)
protocol: Szabályok és eljárások összessége, amik a kommunikációs egységek közötti információcserét felügyelik. (lásd még network protocol)
PSTN: Public Service Telephone Network. (nyilvános szolgáltatású telefonhálózat)
PTT: Post, Telegraph and Telecommunications
Public key: (nyilvános kulcs) Az aszimmetrikus titkosításnál az a kulcs, ami a személyes kulcs párja. Az üzenet küldője ezt közli a többiekkel, hogy lehetővé tegye nekik az általa küldött, privát kulccsal titkosított biztonságos üzenetek elolvasását. **public-key cryptosystem: (nyilvános kulcsú titkosítás)** Titkosító rendszer, ahol van titkos kulcs (secret key), és van nyilvános kulcs (public key). A nyilvános kulcsokat minden felhasználó ismeri. A titkos kulcsokat csak a tulajdonosaik

ismerik. üzenet küldésekor a felhasználó a saját titkos kulcsát és a címzett nyilvános kulcsát használja titkosításra. (lásd Rivest-Shamir-Adleman cryptosystem, RSA).

Q

QoS - Quality of Service: Az Interneten használt protokollok többsége a “best case” elvre épül és nem nyújt semmilyen minőségi garanciát. A QoS garanciákat támogató rendszerek ezzel szemben támogatják a minőségi paraméterek biztosítását, mint a késleltetés, az elveszett csomagok aránya és mások.

R

RAID (Redundant Arrays of Inexpensive Discs): redundanciára épülő diszk alrendszer megoldás. Több verziója létezik. A diszk tömb egy diszkjének meghibásodása RAID megoldás esetén nem feltétlenül jár adatvesztéssel, emellett a RAID eszközökből felépített diszk tömb hatékonyan biztosítja a redundanciát, és az egyes diszkek sebességénél nagyobb sebességű hozzáférést tesz lehetővé a teljes diszk tömb tekintetében.
RAM - Random Access Memory.
RFC - Request For Comments.
RFI - Request For Information.
RFP - Request For Proposals.
RISC - Reduced Instruction Set Computing.
RBT: remote batch terminal (távoli terminál) Egy olyan terminál, amely távol van attól a számítógéptől, amihez kapcsolódik. Ez a terminál a kötegelt feldolgozáshoz gyűjt adatokat, és a kötegelt feldolgozásból vissza is kap adatokat.
real time: információ feldolgozás, amit annak jelentkezésekor rögtön végrehajtanak.
Rejtjelezés: Minden olyan tevékenység, eljárás, amelynek során valamely adatot abból a célból alakítanak át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon. A rejtjelzés részét képezi a rejtjelzett adat eredetivé való visszaállítása is. Nem minősül rejtjelzésnek a személyi vagy objektumazonosítás céljaira szolgáló kódolás, továbbá az automatikus rendszerek mérési vagy vezérlési adatainak kódolása akkor sem, ha az védelmi célokat szolgál. (Magyar Köztársaság 43/1994. kormányrendelete)
Rejtjelezett szöveg (cipher text): A Rejtjelezés eredménye, a védett, olvashatatlanná tett adat,a nyílt szöveg algoritmikusan átalakított megfelelője. Megfejtéséhez a kulcsra, vagy alternatív algoritmusra van szükség.
reliability: (megbízhatóság) A hatékonyság mértéke. Az az időtartam, amíg fogadóképes volt a rendszer, vagy az az átlagos tranzakciószám, amennyi végrehajtható anélkül, hogy hiba merülne fel.
Replika: Egy adatbázisról tetszőlegesen sok speciális másolat készíthető különböző földrajzi helyen elhelyezkedő szervereken, mobil munkaállomsákon. Ezeket a másolatokat hívják replikáknak.
Replikáció: Két replika másolat között az adatok módosításai kicserélődnek, tehát kétirányú adatcsere. Eredményként mindkét oldalon található adatbázis egyforma lesz. Ezt a folyamatot nevezzük replikációnak. A replikáció folyamatával biztosítja a rendszer az elosztott adatbázisok konzisztenciáját. A replikációt: szerver-szerver között a rendszergazda állítja be, ami ezután automatikus; szerver-munkaállomás között mindig a felhasználónak kell kezdeményezni.
response time: (válasz idő) A terminál számára beállított időtartam, amin belül a távoli ellenőrző számítógépes rendszertől választ kell kapnia.
retail banking: (lakossági bankműveletek) A bank tevékenységének az a része, amikor a lakossági számlabirtokosok részére szolgáltatásokat nyújt fiókjaiban.
RFC - Request For Comments: 1969 óta létező fogalom, különböző dokumentációk sorszámozott

tára. Ezen dokumentációk tekinthetők az Internet széles körben vett szabványainak. Valójában ezek nem szabványok, valódi Internetes szabvánnyá nem mindegyik válik és számos RFC nem is tartalmaz szabvánnyal kapcsolatos gondolatokat, csak szervezési alapelveket. Bővebben: RFC 2026 "The Internet Standards Process -- Revision 3".
risk management: kockázat kezelésért felelős részleg vagy tevékenység
Rivest-Shamir-Adleman (RSA) cryptosystem: Nyilvános kulcsú titkosító rendszer, ahol a nyilvános kulcs (public key) és a saját v. egyéni kulcs (private key) nagyon nagy prímszámok szorzatából származnak. Ez a titkosítás aszimmetrikus formája, mindkét kulcs alkalmas titkosításra, amit a privát kulccsal titkosítanak, az a hozzá tartozó publikus kulccsal fejthető meg, és fordítva. (Lásd még bővebben asymmetric key cryptography.)
Router, útvonalválasztó: Az OSI hálózati modelljének 3. rétegét érintő hálózati eszköz, útvonal-irányító és csomagszűrő: Az adatcsomagokat TCP/IP szinten elemzi és a megfelelő irányban küldi tovább, vagy dobja el. Az irányítás folyamata maga több logikára épülhet, így biztonsági problémákat is rejthet magában.
RSA: R. Rivest A. Shamir és L. Adleman által feltalált Nyilvános kulcsú rendszer, az SSH protokoll, illetve például a PGP bizonyos verziói tartalmazzák, kulccsere protokollként a Tunnel Vision és a FreeS/Wan is használja. Legyen a nyilvános kulcs e, m, a titkos d, m az üzenet x. A rendszer alapja hatványozás modulo m, ahol m =p*q két nagyjából azonos méretű prím szorzata. A titkos kulcs a nyilvános kulcsból csak a prímek ismeretében számítható. Ha m elég nagy, akkor faktorizálása elfogadható idő alatt nem lehetséges. A két kulcs kapcsolata; e*d=1 modulo (p-1)*(q-1). A rejtjelzett üzenet y= x e.dik hatványon, míg a megoldó transzformáció x= y a d. hatványon. A két kulcs közötti reláció biztosítja, hogy x= x.

S

Search Engine (Keresőmotor): Olyan interneten található számítógép, illetve azon futó programok, melyek bizonyos időközönként automatikusan feltérképezik a World Wide Weben található több milliárd Website-ot, és kigyűjtik, majd adatbázisba rendezik az ott található kulcsszavakat. A felhasználók ebben az adatbázisban kereshetnek kulcsszavak szerint, a találatokat pedig Hypertext formában kapják meg. A legnépszerűbb keresőmotorok: AltaVista, Google, Excite, Infoseek, Lycos, Magellan, Yahoo stb.
Secret key: (titkos kulcs): A szimmetrikus titkosító algoritmusban használt kulcs, ahol ugyanazt a kulcsot használják a titkosításhoz és a visszafejtéshez.
SEPP: Secure Electronic Payment Protocol
Server: (szerver) Egy számítógép, ami hálózaton (LAN, vagy Wide Area Network) keresztül kiszolgál más számítógépeket.
Session: Egy adott Felhasználó bejárása egy Website-on. A mérték megegyezik a Látogatás mértékkel, azzal a különbséggel, hogy ha valaki megszakítja a böngészést az adott Website -on (tehát kilép az adott Weboldalról, vagy a Böngészőből), akkor a Session befejeződik. Ha később bármikor visszatér, akkor új Session kezdődik. A Magyar Internet Audit Tanács szabványa szerint ugyanannak a Felhasználónak megszakítás nélkül kiszolgált, Website-on belüli Page Impression sorozat.
SET (Secure Transaction Layer): A SET egy olyan elfogadott elektronikus fizetési protokoll, amelyet a Microsoft, a Visa és a Mastercard közösen javasolt.
SET: Secure Electronic Transactions (biztonságos elektronikus tranzakció) A VISA, a MasterCard és még sok más világcég közösen fejlesztette ki. Minden félnek biztonságot nyújt titkosítással, aki nyílt hálózatokon keresztül (pl. Internet) részt vesz a tranzakciókban.
Set-top box - IRD (Integrated Receiver Decoder), digital box. – A digitális, kábeles, műholdas tv-szolgáltatások dekódolását és analóg jellé alakítását végzi.
Smart card: (intelligens kártya) Intelligens kártya, ami képes információt tárolni és feldolgozni. A kártyába épített integrált áramkörök (chip) esetenként jelentős információtároló kapacitások révén

nemcsak információtárolást, de annak védelmét és bizonyos műveletek elvégzését is biztosítják. Egyes változatai saját áramforrással rendelkeznek. A mágnescsíkot tartalmazó banki vagy hitelkártyához képest sokoldalú, aktív kártyának is nevezik. Egy műanyaglapkán elhelyezett integrált áramkörbe zsugorított miniszámítógép mikroprocesszorral, operációs rendszerrel, csak olvasható és olvasható-írható memóriával. Lásd még chip card.
SME - Small and Medium Enterprises: Kis és közepes méretű vállalkozások.
Socks: A Socks egy általanos célú proxy megoldás, gyakorta használját proxy alapú tűzfal környezetben vagy tűzfal kiegészítéseként. A Socks-ot támogató szoftverek, kliensek segítségével a tűzfalon keresztül gond nélkül nyitható bármilyen engedélyezett TCP vagy UDP összeköttetés.
Splash page – Olyan Felbukkanó ablak, amely a hirdető Website-ját tartalmazó ablak becsukása után automatikusan nyílik meg. Használata erőszakos, behatoló, ritkán alkalmazzák.
SSH - Secure Shell: Biztonságos shell elérést biztosító program. kódolja az egész jelfolyamot, így a felhasználók tevékenysége lehallgatás ellen védett.
SST: self-service-terminal, önkiszolgáló terminál általános információk lekérésére
stateful inspection (SI): a hybrid tűzfalak legismertebb képviselője
Sub Level Domain (SLD) – Egyes országokban az országot azonosító Legfelső Szintű Domain Nevek (TLD) alatt meghatároznak az egyes gazdasági szektorokra utaló neveket is, pl. .co=vállalati szféra, .tm=márkanevek stb. (Pl.: www.cegnev.co.hu, www.markanev.tm.hu)
super-smart card: (szuper intelligens kártya) Olyan intelligens kártya, ami tartalmaz egy billentyűzetet és egy vizuális képernyőt, lehetővé téve a felhasználónak, hogy közreműködjön a kártyán belüli feldolgozási funkciókkal.
SWIFT: Society for Worldwide Interbank Financial Telecommunication. (globális bankközi pénzügyi telekommunikációs társasáe;g) Világszerte több mint 1000 bank tulajdonában lévő kommunikációs mechanizmus, amit pénzátutalásra, utasítások és adminisztratív üzenetek továbbítására használnak.
switching: (kapcsolás) Technikai kifejezés. Kapcsolat létesítése és megszüntetése egy kommunikációs hálózatban.
symmetric key cryptography: (szimmetrikus kulcsú titkosítás) Ugyanazt a titkos kulcsot (secret key) használják a titkosításhoz és a visszafejtéshez.
synchronous data network: (szinkron adat hálózat) Adat kommunikációs hálózat, ahol az adatok egyidejűleg továbbítódnak a hálózat láncszemein.
synchronous: (szinkron) Bitek sorozatának egyidejű átvitele.
system network architecture: (hálózati rendszer architektúra) Az IBM számítógépek szabadalmazott hálózati architektúrája.

T

Tanusítvány (Certificate): Egy adott partnerhez tartozó igazolás, ami a nyilvános kulcsát, nevét, lejárati időt tartalmazza, amelyet egy erre felhatalmazott, megbízhatónak tekintett harmadik fél (trusted third party, TTP) a saját nyilvános kulcsával aláírt, s ezzel az adott partner és a nyilvános kulcs összetartozását mindenki számára ellenőrizhető módon hitelesítette. További problémákat vet fel a TTP aláírásnak hitelessége: neki is rendelkeznie kell egy tanúsítvánnyal, amit valaki hitelesített és így tovább.
TCP/IP stack: Az internetes adatátvitel protokolljai az OSI által definiált rétegszerkezethez hasonló egymásra épülő rendszert alkotnak. Ennek a rendszernek jó részét Linux operációs rendszerben a kernel kezeli. A TCP/IP hierarchiát nevezzük TCP/IP stacknek. Ezzel arra is utalunk, hogy valamely protokoll adatát elküldve az végigmegy a hierarchia összes alsóbb rétegén.
TCP: RFC793, RFC1122 és RFC2001 által specifikált Internet-protokoll, Transmission Control Protocol. Széleskörűen használt protokoll, a legtöbb internetes megoldás, mint a www, smtp, ftp ezt használja. Kapcsolatorientált, és garantálja az elveszett adatok újraküldését valamint a sorrend megőrzését.

Teleház: Már magyarországi projektekben is szereplő olyan számítógépekkel és netes kapcsolattal rendelkező nyilvános épület, amelyet mindenki használhat. Általában non-profit intézmény, de ha a posta alakítja ki akkor lehet profitorientált is.(Posta-ház)
Telekommunikáció - 1. Távközlés – adat (szöveg, számok, hang és kép) elektronikus *átvitele* valamely távolságra. 2. Távközlés vagy telekommunikáció: minden *folyamat*, amely bármely alkalmas formájú információ (nyomtatott másolat, álló vagy mozgó kép, látható vagy hallható jelek stb.) továbbítását szolgálja az adótól egy vagy több vevő felé, bármilyen elektromágneses rendszer (vezetékes elektronikus átvitel, rádió, optikai átvitel, csőtápvonal stb.) útján. Ide tartozik a távíró, telefon, videotelefon, adatátvitel stb. Az angolszász irodalomban a telekommunikáció mellett az adatkommunikációs, rádiókommunikációs ágazatok megnevezései is szerepelnek. A magyar szaknyelvben van még egy szó, a hírközlés, melyet szélesebb értelemben használnak, mint a távközlést. 3. Távközlés: *tevékenység*, melynek során bármely értelmezhető jel, jelzés, írás, kép, hang vagy bármely természetű egyéb közlemény villamos vagy optikai úton, rádión vagy más elektromágneses rendszereket megvalósító közcélú, zárt célú, külön célú, saját célú és zárt láncú távközlő hálózatokon, illetőleg ezek kombinációján eljuttatható egy vagy több igénybe vevőhöz, felhasználóhoz.
Telemarketing: áruk, vagy szolgáltatások eladása telefonon keresztül úgy, hogy a kártyabirtokos megadja a pénzügyi tranzakciós kártyája azonosító számát a fizetéshez.
Telematika - 1. Telekommunikáció-informatika: nyilvános információs szolgáltatások: a távközlés, a számítógép és a műsorszórás konvergenciájának eredménye, alkalmazása. 2. Teleinformatika: a "non-voice" szolgáltatásokat meghatározó terminusok, amelyek főként a számítástechnika és a távközlés integrációja alapján működnek.
Teljes kipróbálás: brute-force:Teljes Rejtjelző rendszerekkel szemben alkalmazott támadási kipróbálás mód. Lényege, hogy néhány Nyílt:Rejtjeles pár és a rejtjelző rendszer ismeretében az összes lehetséges kulcsot kipróbálva határozzuk meg az alkalmazott kulcsot. Természetesen a módszer csak akkor végrehajtható, ha a kulcstér mérete egy bizonyos méretnél kisebb.
terabyte: trillió byte
terminal access control: (terminál hozzáférés ellenőrzése) Intézkedések, amik biztosítják, hogy a terminálhoz való hozzáférés csak az engedélyezett személyek számára legyen lehetséges.
terminal emulation: A központi géphez közvetlenül kapcsolt terminált utánzó mikrocomputeres program, ami egy kommunikációs program segítségével működik.
terminal: (terminál) Egy eszköz, ami lehetővé teszi a felhasználónak, hogy a távolból adatokat küldjön, és fogadjon, és hogy egy távoli számítógép funkcióit használja.
third-party processing: (harmadik fél általi feldolgozás) Tranzakciók feldolgozása egy szerződött partner által.
Titokmegosztás: A titokmegosztás alapfeladata az, hogy adott titkot osszunk fel n ember között úgy, hogy közülük bármelyik képes legyen a titkot visszaállítani, de bármelyik-1 még nulla információval rendelkezzen a titokról. A valóságban ennél sokkal bonyolultabb feltételrendszerek is előfordulnak.
Top Level Domain Name (TLD): Legfelső Szintű Domain Név, a domain név legutolsó tagja. Jelenthet országhivatkozást, pl.: .hu=Magyarország, .us=Egyesült Államok, de az Egyesült Államokban jelentheti a szervezet típusát is, pl.: .edu=oktatási, .gov=kormányzati, .com=kereskedelmi)
touch screen: Interaktív, vizuális kijelző eszköz, amit a felhasználó úgy kezel, hogy megérinti a képernyőt, és ezzel kiválaszt egy lehetőséget a kijelzett menüből. Az ilyen képernyők a köré elhelyezett infravörös érzékelőkkel érzékelik az ujj pozícióját.
TPC/IP (Transfer Control Protocol/ Internet Protocol): Az a szabvány, amellyel az interneten különböző rendszerek és számítógépek összekapcsolódnak.
Transaction processing: (tranzakció feldolgozás): Számítógépes művelet, ami a tranzakciók real-time, on-line feldolgozását végzi.
Tűzfal (Firewall): Olyan köztes számítógép, amely a belső hálózatot védi a külső behatolásoktól. Ezáltal biztonságosabb a rendszer, és a hálózati kommunikáció. Tűzfalakkal egyes hálózati részeket

védenek az Interneten. A tűzfalaknak számos típusa és a védekezésnek változatos módozatai léteznek. A tűzfalak általában szűrnek, azaz csak bizonyos adatokat engednek át, és biztonsági okokból speciális célszoftvereket alkalmaznak a különböző protokollok adatainak átvitelére. A tűzfallal védett hálózatból kifele illetve a hálózatba befele nem lehet mindig mindent elérni, ezért ez egyes esetekben gondot okozhat.

U

UDP: Az User Datagram Protocol az Internet egyszerű protokollja, segítségével gyors adatcsere valósítható meg. Az UDP adatátvitel esetén nem épül ki csatorna a két végpont között, így nem garantált, hogy az elküldött adatok nem vesznek el, illetve az is előfordulhat hogy az adatok nem az elküldés sorrendjében érkeznek meg. Speciális célokra az UDP átvitel hatékonyabb a TCP-nél.
UMTS - Universal Mobil Telecommunications System.
Uniform Resource Locator (URL): Magyarul egységes forrásazonosító, a World Wide Weben használt címzési szabványrendszer, megadja az információ elérésének módját, és az információ pontos helyét a távoli számítógépen. (pl: http://www.adage.com/index.html) ld. még: Domain-név
UNIX - Elterjedten használt számítógépes operációs rendszer, melyet eredetileg a Bell Laboratories-nél fejlesztettek ki 1969-ben. Az Interneten már a Berkeley UNIX terjed el, amely az eredeti 7. változatából származik. 1974-ben publikálták nyilvánosan és 1979-ben került kereskedelmi forgalomba. További változatai is vannak. A kilencvenes évek vége felé a Windows NT komoly vetélytársa lett számos területen.

V

VAN - Value-Added Network: Értéknövelt hálózat.
VAN - Video Access Node: Videokonferencia-rendszer.
VSAT - Very Small Aperture Terminal – Az egyedi műholdas távközlés eszköze.
very large scale integration (VLSI): A funkciók nagyon nagy fokú integrációja. Egy szilikon chip-be nagy számú alkotóelem beépítése. (ritkán használt kifejezés)
VIDEOTEX - Interaktív elektronikus szolgáltatás egyéni, otthoni, hivatali vagy nyilvános használatra. A videotext szöveget, képet és hangot is tartalmazhat. A felhasználó maga is közölhet információt és távoli tranzakciókat végezhet. A helyi BBS-ek és az Internet-szolgáltatás is megjelenhet. A MATÁV külön szolgáltatásként üzemelteti a 80-as évek vége óta videotext-rendszerét. Lásd *interaktív elektronikus szolgáltatások.*
Virtual Shopping Mall: (virtuális bevásárló utca) Egy olyan bevásárló utca, ami a virtuális térben van, és sokféle kereskedőt gyűjt össze. (Internetes bevásárlóközpontok)
Visit (Látogatás): Ez a mérőszám definiálja az egy Weboldalt meglátogatók számát. Ez egy abszolút értéket ad a kapcsolatfelvételekről (rákattintásokról), de anélkül, hogy az új és a visszatérő látogatókat egymástól meg tudná különböztetni. A Visit egy olyan Page Impression sorozat, melyet egy Felhasználó "generál". A Page Impression sorozat akkor kezdődik, amikor a felhasználó megtekinti az első, az adott Website-ról származó oldalt, és akkor fejeződik be, amikor legalább 30 perc szünet van két, ugyanennek a Felhasználónak kiszolgált Page Impression között. Tehát ha a felhasználó elmegy az adott Website-ról, és 30 percen belül visszatér, akkor az egy látogatásnak számít. Ha a gépén "nyitva hagyja" az adott oldalt, és nem kattint sehová 30 percig, majd visszatér, és újra elkezd böngészni az oldalon, ez két látogatásnak minősül. A Magyar Internet Audit Tanács szabványa szerint egy Felhasználónak kiszolgált Page Imression sorozat, mely akkor ér véget, amikor legalább 30 perc szünet van két, ugyanennek a Felhasználónak kiszolgált Page Impression között.
Visitor (Látogató, Felhasználó): Egy adott Látogató alatt egy adott IP címet értünk, azaz egy olyan számítógépet, ahonnan egy vagy több személy böngészi az internetet. Ez a számítógép

közvetlenül csatlakozik az internetre. Egy IP címhez (számítógéphez) több számítógép, illetve Felhasználó is tartozhat, amennyiben az internetre közvetlenül csatlakozó számítógép egy központi szerver. A modemen keresztül csatlakozó felhasználók minden internetre kapcsolódáskor más IP címet kaphatnak a központi szervertől. A fenti okok miatt csak a Látogatások és a Látogatók számát lehet pontosan megmondani, az, hogy a látogatások "mögött" hány valós személy található, csak becsléssel vagy utólagos kutatással állapítható meg.
visual display unit: (képernyős megjelenítő eszköz) Számítógép kimeneti eszköz, ami a felhasználónak alfanumerikus, vagy grafikus adatokat jelez ki egy frissíthető képfelületen.
VOD - Video-On-Demand – Igény szerinti hálózati video: mintha a felhasználó saját VCR-ét használná, de a szolgáltató bő listájáról választhat a távolból.
VPN: Virtual Private Network, virtuális magánhálózat. Egy nyilvános hálózaton létrehozott másodlagos, virtuális hálózat, amely egy cég magánhálózataként funkcionálhat. Jellemző példája egy az Interneten létrehozott céges belső hálózat, amely titkosítva és autentikálva továbbítja az adatokat a cég telephelyei között.

W

WAN (Wide Area Network): Szélesebb körű sokgépes hálózat (nagy távolságú hálózat), gyors adatátviteli lehetőséggel
WAP (Wireless Application Protokol): A WAP technika egy napjainkban gyorsan fejlődő kommunikációs protokoll, ami lehetővé teszi szöveges és képi információk megjelenítését mobiltelefonokon. Ennek segítségével lehetővé válik az internet böngészése mobiltelefonon keresztül.
Web, WWW: World Wide Web, az Internet legismertebb és leggyorsabban fejlődő alkalmazása. A képernyő tartalom (kép/szöveg) szerint kiválasztott pontjára mutatva és kattintva (hipertext) a kívánt információt tartalmazó – szöveg, kép hang – oldalhoz jutunk. A World Wide Web hatalmas mennyiségű témát kínál a világból. Az információ átvitele a HTTP protokollon keresztül történik.
Webpage (Weboldal): Honlap, a tulajdonos World Wide Web belépési pontja, amely általában további érdeklődés szerinti témákra való ugrást kínál. Egy olyan dokumentum, amely a Böngészőben egy oldalként jelenik meg. Tartalmazhat szöveget, Hyperlinkeket, képet, hangot, animációt, videót, illetve aktív, az oldal megjelenésekor elinduló programot is.
Website (Honlap): Általában az egy elérési cím (Domain) alatt található, egymással szoros kapcsolatban lévő Web-oldalak együttese.
World Wide Web: összekapcsolt szerverek (Web oldalak) hálózata az interneten, amit egy keresővel (pl. Netscape Navigator, Internet Explorer) el lehet érni. A web oldalak tartalmazhatnak szöveget, grafikát, videót, és hangot is.
WORM: Write Once Read Many Times. (egyszer írható, sokszor olvasható) A CD-ROM változata.