Kriptográfia vizsga

Pici doksika, amiben összegyűjtöttem szépen elrendezve a cuccost, amit Csapodi elvárna a vizsgára, és elküldött emailre. Mivel ezek a források szerintem picit kaksik beletettem ilyen szép zölddel, amit én hasznosnak érzek a témában. És a végén van egy vizsga tapasztalat gyűjtemény is a leírtak alapján

Néhány hasznos link:
Haktás összefoglaló 1: https://users.itk.ppke.hu/~hakta/segedanyagok/6-szemeszter/Kripto/kripto_Leichner.pdf
Haktás összefoglaló 2: https://users.itk.ppke.hu/~hakta/segedanyagok/6-szemeszter/Kripto/LeichnerD.pdf

ZH1: https://users.itk.ppke.hu/~hakta/segedanyagok/6-szemeszter/Kripto/kripto_zh1_2016.pdf
ZH2: https://users.itk.ppke.hu/~hakta/segedanyagok/6-szemeszter/Kripto/kripto_zh2_2016.pdf

Minden dia egyben: http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/merged.pdf

Előadás felvételek:
https://drive.google.com/drive/folders/1fiv0gusaY6NgAYxTR_Np-5TZ8U9lZmFk?usp=sharing

Matek

Kis fermat tétel bizonyítással

https://primes.utm.edu/notes/proofs/FermatsLittleTheorem.html (ez a bizonyításhoz)
https://mathworld.wolfram.com/FermatsLittleTheorem.html (ez a dolgokhoz)

Euklideszi algoritmus

https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%C3%A1g%C3%89sKriptogr%C3%A1fia/osszefoglalo.pdf (23-26)
https://www.youtube.com/watch?v=JUzYI1TYMcU (ez maga a számolás bemutatása, hogy hogyan kell használni az algoritmust)

Bitcoin

http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-Bitcoin.pdf (előadás)
https://bitcoinbook.info/wp-content/translations/hu/book.pdf (ez kurvahosszú, arra jó, hogy keresni tudsz benne ha valami nem tiszta)
https://www.youtube.com/watch?v=bBC-nXj3Ng4 (ha van időd és érdekel, nagyon szépen bemutatja)

Random

http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-Veletlengeneratorok.pdf (előadás)
https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%C3%A1g%C3%89sKriptogr%C3%A1fia/SP800-90revised_March2007.pdf (7. 8. fejezet 11-23)

Adatfolyam rejtjelezők

Általános osztályozás és LFSR alapú adatfolyam rejtjelezők típusai:

http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Extra/chap6.pdf (192 - 196 alja, 6.3 ábrái)
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-Adatfolyamrejtjelezok.pdf (előadás)
https://www.youtube.com/watch?v=8fhNPXus4-s (LFSR-t tűrhetően bemutató vidike)

GSM

http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-GSMSecurity.pdf (előadás)
Rizsához ajánlott:
https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%c3%a1g%c3%89sKriptogr%c3%a1fia/Introduction_gsm_security.pdf
https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%c3%a1g%c3%89sKriptogr%c3%a1fia/10.1.1.465.8718.pdf
https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%c3%a1g%c3%89sKriptogr%c3%a1fia/jensen_andersen.pdf
https://www.youtube.com/watch?v=LgZAI3DdUA4 (A5/1 animáció)

WEP/WPA

https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%C3%A1g%C3%89sKriptogr%C3%A1fia/benton_wireless.pdf (16-24)
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-WEP_WPA.pdf (előadás)

DVB

https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%C3%A1g%C3%89sKriptogr%C3%A1fia/Muhammed_Awan_-_DVB_Architecture.pdf (4. fejezet)
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-DVBtitkositas.pdf (előadás)

Diffie-Hellman

https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%c3%a1g%c3%89sKriptogr%c3%a1fia/diffiehellman.pdf (6. oldal “We now suggest”-től fejezet végéig
https://www.youtube.com/watch?v=NmM9HA2MQGI (ez egy nagyon jó szemléletes példa, hogyhogyan működik)
https://www.youtube.com/watch?v=Yjrfm_oRO0w (ebben pedig a matekos részt is elmondja, nem hosszú)
https://www.youtube.com/watch?v=yDXiDOJgxmg (elliptikus diffie hellman)
https://www.youtube.com/watch?v=F3zzNa42-tQ (elliptikus diffie hellman)

RSA

https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%c3%a1g%c3%89sKriptogr%c3%a1fia/rsapaper.pdf (2-6. fejezetek és a 7. fejezet A és D pontja)
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-Nyilvanoskulcsurejtjelezes.pdf (előadás)

Blokk rejtjelezők, DES TDEA

http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Extra/chap7.pdf
https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%c3%a1g%c3%89sKriptogr%c3%a1fia/3DES.pdf (7. fejezet, 7.2 és 7.4 fejezet - ami előadáson is szerepelt belőle)

http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-Blokk_rejtjelezok_2.pdf (előadás)

AES

https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%c3%a1g%c3%89sKriptogr%c3%a1fia/fips-197.pdf (1-5 fejezet)
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-Blokk_rejtjelezok.pdf (előadás)
https://drive.google.com/file/d/1TnkFluChLjX7vFNkUiq-y46AG8nqWUuC/view?usp=sharing (előadás videó)

Műveletek bináris polinomokkal

https://wiki.itk.ppke.hu/twiki/pub/PPKE/Adatbiztons%C3%A1g%C3%89sKriptogr%C3%A1fia/osszefoglalo.pdf (11-12)

Euklideszi algoritmus bináris polinomokkal

Az órán elhangzottak alapján (nem a matek összefoglalóból). ¯_(ツ)_/¯

Elliptikus görbék

https://andrea.corbellini.name/2015/05/30/elliptic-curve-cryptography-ecdh-and-ecdsa/
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Extra/elliptikus_of1.pdf
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Extra/elliptikus_of2.pdf
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-Elliptikusgorbek.pdf (előadás)
https://www.youtube.com/watch?v=NF1pwjL9-DE (jó kis videó)
https://nws.niif.hu/ncd2002/docs/ehu/15/index.html (jó kis összefoglaló a témáról)

PKI és SSL/TLS

http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-PKI.pdf (előadás)
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-SSLTLS.pdf (előadás)
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Extra/PKI_sp800-32.pdf (ez is marha hosszú, max keresésre jó)
http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Extra/PKI_SSL.pdf

SSL/TLS handshake

Ehhez sem adott meg külön anyagot a papó.

SSO

http://users.itk.ppke.hu/~ekacs/anyagok/felev6/Kripto/Eloadasok/eloadas-SSO-converted.pdf (előadás)

Egyéb linkek

https://crypto.stackexchange.com/questions/31899/what-is-difference-between-meet-in-the-middle-attack-and-man-in-the-middle-attac (meet in the middle, man in the middle)

https://www.youtube.com/watch?v=1GoP_HfF_v4 (A5/1, block vs stream)

Vizsgatapasztalatok

Diffie helman, szinkron onszinkorn, ez milyen blokkrejtjelezobol csinálható. Wep, elliptikus diffie helman, fontos h a diffie helman a diszkrét logirtmuson alapszik.. meet in the middlenel csak az arányok, meg h az rsa meg a diffie meg az aesről volt az a táblázat, jó tudni az arányokat. Nagyon rendes volt, amikor elkezdtem mondani, kb ha látta, hogy tudom mi van, be se kellett fejezni. Ja és volt az a5 algoritmus, meg jó ha tudjátok, hogy abban 3 lffsr van. nem is tudtam, h a diffie helman az diszkrét logaritmuson alapszik.

és ő mondta a témákat, vagy megkérdezte h mirol szeretnél beszélni?
aztán kérdezte, hogy mi tetszett, mondom uccu bemondom neki az elliptikusat.
és akkor arról beszéltünk egy kicsit
de valójában ő irányította a témát
szóval mindenből egy kicsit

Kis fermat , diszkret logaritmusos cucc , szinkron onszinkron cuccos ,meet in the middle , ismetelt negyzetre emeles az rsa nal
Csak a lenyege kellett az annyi higy hamarabb elerd nagy hatvanyoknal a megoldast (errol meg valamit az eloadason tolt az elejen mindig)

Elliptikus görbék-összeadás Diffi-hellmann-matematikai háttér(diszkrét log) A8 (igazából A5 bocsi) AES négy művelete Wep-Shared Key Authentication Vulnerability (wep man in a middlelel támadható ha azonos iv-t használsz)

Na én most voltam, Kis fermat, mire használjuk, A5, eliptikus görbe összeadása hogy van folytonos esetben, card sharing támadás DVB-nél, ezt nem tudtam eléggé, de éppen belementem volna a kamuzásba,amikor elment a netje a csávónak, és amikor visszajött akkor mondta h ad egy ötöst :DD

nekem elején kérdezte az elliptikus görbéknél (valósoknál) hogyan lehet 2 pontot összeadni és akk nem a képletes hanem szerkesztős érdekelte, utána kis fermatot hol használjuk, a5, wepnél támadás, meet in the middle kb ez asszem

Kicsit csúsztunk de nem baj ha hamarabb elindítod a cuccost
Első kérdés : Tudok e mindent ? 😀
Második kérdés: A Kis Fermatot biztos tudom, úgyhogy mondjam el
Harmadik : Hol használjuk? (prímteszteknél, az RSA-nál)
4. : Mik a paraméterek mit mibe helyettesítünk (Kis Fermat)?
5. : Milyen módszert használunk arra hogy gyorsan elérjünk egy hatványt ? (imételt négyzetre emelés)
6. : Ezt hol használjuk ? (Diffie Helmann, és egy kicsit erről is kellett mesélni)
7. : Blokkrejtjelezők két osztályozása ? (szinkron, önszinkron)
8. :Ezeknek melyik felel meg OFB, CFB? (szinkron: OFB, önszinron :CFB)
9. : TDES ellen milyen támadás van (Meet in the middle) és a komplexitások ismertetése
10. : Mennyire néztem át a WiFi-t ?
11. :Milyen gyengeségei vannak ? (SKA támadás ha nem titkosított, Checksum, IV ismétlődés)
Ez nem tudom hagyadik volt . : Eliiptikus görbe összeadás művelete

Nem vészes, nem kérdez nehezet, ilyen RSA-t, DES sebezhetőséget,irreducibilis polinomot szokott kérdezni, WEP-t, GSM, véletlen szám generalást, kerberos protokollt. Arra kérdez rá ha valamit rosszul mondazs. Szerintem egy ilyen 3-4-st elég könnyű összeszedni.

az alapokat nagyon
Diffi-Hellman, RSA,
Ad egy példát és azt kell kézzel kiszámolni.
És kellett kis fermat tételt konkrét feladatra alkalmazni

Ezeket tavalyról: (itt volt írásbeli is)

- kis Fermat tétel alapján számolj ki egy nagy hatványt
- ábrázolj egy elliptikus görbét (mint a kis zh-ban)
- adatfolyam rejtjelező blokk diagram
- melyik az erősebb A5/1 2 3
- mi a komplexitása pl a diszkrét logaritmusnak
- melyik használ blokk rejtjelezőt és akkor fel vannak sorolva algoritmusok mint RC4 stb...
- ismertesd az RSA-t. felírod hogy mi a p, q, n, fí, e ,d, ezekből hogy kódolsz, meg dekódolsz.
- Diffie-Hellmann, adott példa, old meg.
- add meg a 4-ed fokú irreducibilis polinomokat.
- ezek közül melyiknek multiplikatív inverze egy megadott polinom

AES műveletei, emv kártyák statikus és dinamikus autentikációi, GSM, A5/1,2,3, PKI

Rsa kérte a bizonyítást is nem tudtam ezért lehuzott egy jegyet

Egy közös írásbeli van. Olyan feladatok voltak benne, hogy az emv kártyák dinamikus autentikációjának az ábráját kellett lerajzolni, elmagyarázni. Aztán egy görbe elliptikus pontjait kellett felrajzolni, és hozzá leírni a Diffie-Hellman kulcsmegosztást elliptikus görbe felett. Ezen kívül fel kellett írni az ötödfokú irreducibilis polinomokat,az AES helyettesítés műveleteit magyarázattal. Meg azt hiszem egy blokk rejtjelezőt is fel kellett rajzolni.
Ezután/közben aki végzett, azt elkezdte szóbeliztetni. Ez abból állt, hogy adott egy témát amit ki kellett dolgozni(ezeket írták fent a többiek). Ezt átfutotta, és ha valami hibás volt, abba belekérdezett. Illetve ha valamit nem tudtál a vizsga írásbelin, abba is belekérdezett.
Szerintem részletesen kell kifejteni, mert ha vázlatosan fejted ki, akkor később belekérdez(bár ez is lehet jó, ha tudod).

Egész számos görbét úgy ábrázolsz, hogy felírod az egész számokat 1-től n-ig, aztán ezeket behelyettesítve x-be megnézed, hogy melyikre kapsz egész y-t. Ezek a pontok tartoznak a görbéhez, illetve a (0,0).