**Új lehetőségek a pixel-alapú kriptográfiában**

Szerzők: Pitlik, László, Pitlik László (ifj.), Pitlik Mátyás

Magyar kivonat:

Előtörténet: Az intézményközi MY-X kutatócsoport már számos[[1]](#footnote-1) minőségi kódolási eljárást dolgozott ki annak érzékeltetésére, hogy kvázi végtelen azon transzformációk száma, melyek alapján bizonyos információk elrejtése lehetséges.

Háttér és benchmark: A közismert Caesar-kód egy rel. kis méretű kombinatorikai teret definiál, mely feltörése rel. könnyű. A Caesar-kód köztudottan betűkre/számjegyekre fókuszál. Azonban a digitalizáció folytán a betűk/számok pixel-mátrixok formájában reprezentálódnak. Vagyis a pixel-mátrix egyes elemeinek kiemelése (felvillantása) lehetővé teszi, hogy az emberi szem a kiemelt pixelek által alkotott jelet valamilyen betűként, számként engedjenek felismerni. Következésképpen egy (pl. bináris) pixel-mátrix (0;1) által leírt betű/számjegy titkosítható, amennyiben a pixelek értéke szabály-alapú transzformáció(ko)n esik át.

Releváns részletek: A pixel-értékekre vonatkozóan újszerű (titkosítási/dekódolási) szabályok alakíthatók ki: pl. egy betű vagy éppen egy tetszőlegesen sok betű által alkotott egység (képrészlet – pl. egy kézírás digitalizált verziója) digitalizált adatsora valamilyen módon úm. körré alakítható, ahol a Caesar-kód-jellegű eltolás, mint transzformáció azonnal értelmet nyer. De természetesen nem csak egyszerű eltolások hozhatók létre, de celluláris automata jellegű szabályok is. Sőt, ezek a szabályok lehetnek olyan komplexek, hogy csak egy irányba egyértelműek, azaz nem dekódolhatók (hacsak nem egy önálló kombinatorika rejtély formájában – vö. pl. aknakereső-szerű logikai kapcsolatok pixelek között). A bináris pixel-értékhalmaz egy-egy kép esetén értelmezhető a genetikus algoritmusok transzformációnak (vö. mutáció, keresztezés) bevonásával is. A kiindulási kép pixel-értékeire vonatkozó transzformációk definiálásába sorozatok (pl. Fibonacci) is helyet kaphatnak, ill. véletlenszámként ható vezérlések (vö. a PI-tizedes jegyei) ismét csak alkalmasak arra, hogy a kiindulási pixel-halmazból szabály-elvű módon kvázi tetszőleges (véletlennek tűnő, de még sem véletlen) hozzárendelési szabályrétegek legyenek kialakíthatók. A pixel-értékek értelmezési intervalluma nem csak bináris lehet, hanem numerikus is (pl. szürkeárnyalatos képek 0-255 közötti értékei). Ezekre a számhalmazokra lényegében tetszőlegesen sokféle transzformációs szabály alakítható ki. A fentebb érzékeltetett pixel-alapú (minőségi) titkosítási lehetőségek elsődlegesen nem a ma ismert, tömegesen használt (mennyiségi) nyílt/titkos kulcsokra alapozó (de)kódolás alternatívái, melyek esetében a védelmet a kombinatorikai tér nagysága és a mindenkori számítási kapacitások közötti jelentős nagyságrendi eltérések adják (vö. kvantumszámítógépek okozta kockázatok). A minőségi (de)kódolás lényege az ötlet egyedisége (vö. adott közösség ABC-jének lecserélése egy új/ismeretlen ABC-re, ill. kevés beszélő által használt (kihaló) nyelvek direkt használata).

Jövőkép: A pixel-alapú titkosítás célcsoportjai leginkább a kis üzenetmennyiséget forgalmazó pl. üzleti partnerek, hiszen pl. így tervrajzok is kódolhatók non-figuratív képként speciális vízjellel támogatva. A fenti gondolatkör természetesen kombinálható minden más ismert elvárással pl. betű-gyakoriságok leplezés, egy betű több helyettesítő jel, stb.)

*Kulcsszavak: celluláris automata, genetikus algoritmus, bináris/numerikus pixel-érték transzformációk, , bináris Caesar-kód-jellegű kódolás, képek (kézírás) kódolása/dekódolása*

Abstract:

History: The trans-institutional MY-X research team produced till now more qualitative ciphering solutions in order to demonstrate the quasi unlimited possibilities of transformations being capable of hiding information (see examples in the footnotes[[2]](#footnote-2)).

Background and benchmarks: The well-known Caesar-codes define a small combinatorial space – easy to identify it. The Caesar-codes are always focusing on letters/numbers/characters. But the digitalisation represents these characters in form of pixel-matrices. Dot-matrix-fonts in dot-matrix-displays let flash certain pixels for a particular letter. Therefore, digital/binary Caesar-codes could be created if the active and passive pixels (see 1;0) would be modified – in a rule-based form.

Highlighted details: The focusing on the pixels of the digitalized letters makes it possible to involve new transformations into the coding-decoding processes: e.g., pixels for one letter or even for arbitrary letters (see an entire picture – where in case of hand-writing-messages the recognition module can also be part of the decoding process) can be transformed into a circle in different ways, where the Caesar-code-like shifting can be interpreted immediately. Not only simple shifting-patterns can be defined, but also rules for cellular automata. These rules can even be so complex, that the decoding is quasi impossible, or this becomes a new combinatorial challenge. The digital representation of letters can also be seen as a door to the genetic algorithms with their specific transformations (like mutation, crossing, etc.). Patterns for binary pixel-values can be created based on different series like Fibonacci or even specific randomized inputs like pi. Digitalized pixel-values can have numeric contents (like in case of grey-scale-pictures). With these numeric values, new (quasi arbitrary) transformations can be initialized. The above-mentioned possibilities are not direct concurrent approaches for the well-known cryptographical solutions (see private/public keys), where the quantities become qualities (in case of limited computational capacities).

Future aspects: The pixel-oriented approaches can rather be compared to the old/rare native languages used e.g., in the second world war e.g., by Americans e.g., against Japanese (c.f. code talkers). Therefore, the above-presented pixel-based approaches can be used in case of specific demands: communication between business partners, agents. These qualitative techniques make possible to hide graphical plans as a kind of non-figurative picture. Specific watermarks can also be created based on pixel-transformations. These solutions can be combined with quasi arbitrary other effects (c.f. letter-statistic-homogenisation, blurred contours of letters, more substitutions for one original input, etc.).

*Keywords: cellular automata, genetic algorithms, binary/numeric pixel-value transformations, binary Caesar-code-like ciphers, de/coding of pictures (hand-writing messages)*

# Bevezetés

A titkosítás, mint az emberiség kezdeteitől ismert kihívás szakirodalma széleskörben, ill. nagy mélységig taglalja ezen szakterület mibenlétét. Ezen cikk szempontjából az újszerű kódolási megoldások természetesen beleilleszkednek a titkosítás történetét eltérő logikák mentén feldolgozó mintázatokba, hiszen már a cikk címe, a pixel-alapúság is a betű/számjegy-alapúsághoz képest definiálja önmagát, s egyben azonnal jelzésre is kerül, hogy kvázi minden ismert trükk integrálható ezen újszerű megközelítésbe.

A cikk tehát értelmezhető a titkosítás leíró szempontjai alapján, de sokkal inkább érdekes, hogy a pixel-alapúság kapcsán összekapcsolásra kerüljenek egymással látszólag távoli fogalmak: mint pl. a celluláris automaták, a genetikus algoritmusok, a mesterséges intelligencia, a szépség fogalmai/megközelítései.

Emellett a (minőségi) újszerűségre törekvés olyan oktatásmódszertani iránymutatás, mely egyszerre lehet képes kondicionálni pl. a programozás kapcsán érdeklődőket, hiszen az innovativitás kényszere (vö. a kvázi végtelen lehetőségi téren belül egy-egy saját konkrét variáns paramétereinek meghatározása), majd a tervparaméterek alapján átlépés a KNUTH-i univerzumba, azaz a valós rendszer (kódoló és dekódoló szoftver megalkotása) didaktikailag érdekes kihívásként hathat akár tömegesen is az informatika iránt érdeklődő pl. Hallgatók számára. De akár a pedagógus-továbbképzés kapcsán is a magolás-orientált történelmi hagyományok ilyen erőterek mentén tolhatók el a kompetencia-alapú oktatás irányába. Ahol a titkosítás (mint a gamification egy speciális formája) önmagában is rendelkezik egy fajta varázslat-jellegű légkörrel…

Jelen dokumentum angol nyelvű verziója már előadásra és megjelenésre került: 6th International Congress on Scientific Research August 18-20. 2023, Ankara by IKSAD Institute[[3]](#footnote-3)

# Előzmény-projektek

Itt és most kerüljön kiemelésre a kutatócsoport múltjából három [1-2-3], egymástól karakteresen különböző, mégis a bevezetésben leírt céloknak párhuzamosan megfelelni akaró projektaktivitás a részletes dokumentációk kivonatai alapján:

1. Telefon-projekt[[4]](#footnote-4) [1]
2. Szépség-projekt[[5]](#footnote-5) [2]
3. ZH-javítókulcs-feltörő projekt[[6]](#footnote-6) [3]

[1] Az első gondolatkör a telefonok számjegy-orientált, de betűket is reprezentáló billentyűzetének specialitásait felhasználva dolgozott ki kódoló és dekódoló megoldásokat:

*„A titkosírások története számtalan megoldást ismer és vélelmezhetően végtelen sok trükk alakítható ki szövegek a triviális olvashatóságának nehezítésére. A három részes cikksorozat első részében bemutatandó kódoló, majd a második részben prezentálandó dekódoló eljáráshoz az alapötletet a mobiltelefonok tárcsázási logikája adta, ahol egy gombon több betű is elhelyezkedik. A harmadik rész a kódoló program finomhangolásáról szól, vagyis a kezdő és a haladó programozók szemlélet-különbségei kerülnek példa-értékűen bemutatásra. Egy rel. nehéz titkosírás esetén elvárható, hogy a szavak határát ne lehessen felismerni, ill. az is elvárható, hogy egyes betűket/jeleket ne csak egy jelsorozat helyettesítsen, ill. lehetőség szerint legyen a titkosírásban értelmetlen/zavaró jelből is valamennyi – minél inkább véletlenszerűnek tűnő módon, sőt egy-egy üzenet ne azonos jelsorozattá alakuljon a titkosítás során mindenkor lehetőség szerint. A mellékelt titkosító demo egy C++ állomány, melyet a repl.it oldalon lehet futtatni. A cikk tartalmaz demo-üzeneteket is a titkosítási folyamat input-output-viszonyainak demonstrálására.”[[7]](#footnote-7)*

*„A KNUTH-i elv[[8]](#footnote-8) értelmében dekódolásról akkor beszélhetünk, ha a teljes folyamat programozott képességként kerül felkínálásra. Vagyis az, hogy emberi intuícióval (találgatással) adott üzenet megfejtettnek minősül, még nem felel meg annak az elvárásnak, hogy a dekódolás hibátlanul képes futni automatikusan. Jelen cikk egy három részes sorozat második eleme, ahol az első cikk a titkosítási eljárást már bemutatta. Itt és most a visszafejtő/dekódoló program kerül bemutatásra, míg a harmadik cikk a kódoló/titkosító eljárás finomhangolásának elvi és gyakorlati vonatkozásait mutatja be. A cikksorozat célja a gamifikált tanulás támogatása.”[[9]](#footnote-9)*

*„A titkosító eljárások készítése során a programozó előbb-utóbb belefut a kód hatékonyságának kérdéskörébe. Hiszen a nagy mennyiségű szövegek átkódolása nem igényelhet tetszőlegesen sok időt valós üzenetváltási folyamatokban, ahol még a kommunikáció maga is időigényes lehet, ill. a kommunikáció zavarása miatt az időigény eleve jelentősen megnőhet. A kódhatékonyságot sokféleképpen lehet növelni. A cikksorozat harmadik, s egyben befejező részében a laikus és a profi kódolás közötti szemléleti/stratégiai és operatív szempontok kerülnek felvillantásra.”[[10]](#footnote-10)*

[2] A második projekt kulcsszava a szépség matematikája. Ennek direktben még nem kell, hogy köze legyen a titkosításhoz, de az az adatvagyon, ahogy egy kép pixel-grafikusan és pixelei szomszédsági viszonyai formájában értelmeződik a mesterséges intelligencia számára, már megnyitja a pixel-alapú transzformációk (vagyis a titkosítás) felé az utat (vö. szteganográfia[[11]](#footnote-11)):

*„Az aranymetszés a természet formavilágának egy karakteres arányára (phi=1.618) mutat rá. A szépség matematikáját firtató kutatás célja ezzel párhuzamosan a robotszemek számára egy olyan mesterséges szépség-skála alkotása (itt és most egy nonfiguratív tesztkép és egy random pontokból álló kép összehasonlítására támaszkodva), mely skála alapján egy robot különbséget tud tenni context-free módon (vagyis a mindenkori kép potenciális tartalmától függően) szép és csúnya, szebb és még szebb között. Vagyis a szépség matematikájától annyit várunk, hogy átmenjen a Turing-teszten és mindennemű speciális esztétikai képzés nélkül, tanulást támogató kép-adatbázis nélkül, korábbi emberi értékítéletek ismerete nélkül, vagyis már egyetlen egy képről is vélelmezni tudja, hogy (koncepciózus) műalkotás-e, vagy inkább a véletlen (koncepciótlan) terméke. Ezen skála megteremtése matematikailag egyszerű, mert a skála eredete a kockázat context-free fogalmára vezethető vissza, ahol minden adatpont kockázatos, mely a többi adatpont (az adatpontok egymáshoz képesti hasonlóságai) alapján nem becsülhető tetszőleges pontossággal. A skála melléktermékeként is tekinthetünk a robot-esztétára, aki nem más, mint egy-egy kép kapcsán a leginkább kritikus pixelek, foltok kijelölésére alkalmas, vagyis a kompozíciót racionálisan (s ismét csak nem véletlenszerűen) kritizálni képes mesterséges intelligencia-alapú eljárás. A robot-esztéta operatív működését úgy lehet elképzelni, mint a kevésbé jól éneklő ember hangfelvételét az ideális hangmagasságokhoz korrigálni képes eljárás, ahol az ideál a képpontok közötti matematikai harmónia maga.”[[12]](#footnote-12)*

*„A robotesztéta elméleti bemutatását kínáló I. rész után, ebben a cikkben egy valós Turing-teszt-folyamat kerül dokumentálásra. A véletlenszerűen választott 15 nonfiguratív (modern) képet véletlenszerűen választott 36 tesztelő személy értékelte 1<10-es szépségskálán színes és szürke verzióban külön-külön. Az elemzés első kérdése az volt, vajon képesek vagyunk-e hasonlóságelemzési alapon skálát építeni a véletlenszerű szépség-értékeléstől való képenkénti különbségtételre. Vagyis képesek vagyunk-e a szignifikancia fogalma nélkül kijelenteni, vajon melyik képről alkotott emberi vélemény mennyire különbözik a véletlentől? Melyik különbözik a legkevésbé? Melyek különböznek norma alatti módon, ill. melyik különbözik leginkább? Ezt követően levezetésre került egy fajta statisztikai aggregált szépség-index ismét csak hasonlóságelemzési, ill. naiv (nem optimalizált) alapon a kapott emberi szépség-pontok leíró statisztikái alapján. Mindezzel párhuzamosan létrehozásra került a legegyszerűbb robotszem, mely naiv módon abból indult ki, hogy egy adott pixel szürkeárnyalatos értékét az alapkép szóban forgó pixelt körülvevő pixeleinek szürkeárnyalatos adatainak átlaga racionálisan képes leírni. A becsült kép és a valós kép eltéréseiből számos statisztikai leíró mutatót számolva, hasonlóságelemzéssel létre jött az aggregált szépség a robotszem által érzékelve, ahol szép az, ami minél inkább mintázatszerű – jelen esetben naiv mintázatokat követő. Az eredmények alapján egyrészt kijelenthető, hogy 15-ből csak 3 képről illik humán szépség-ítéletet formálni az erősen szóró, vagyis véletlenszerűséghez közel álló nyers pontok és a bármilyen okból invaliddá váló modell-részeredmények kapcsán. Az elméleti részhez képest egyelőre még csak naiv mintázatokkal dolgozó robotszem és a humán értékítéletek egyetlen egy ponton közösek, vagyis egy képről nagy biztonsággal állítható, hogy rel. csúnya a többihez képest. A humán szépség-fogalom véletlenszerűsége kapcsán a Turing-teszt csak annyiban tekinthető sikeresnek, hogy az egy közös horgonypont létezését sikerült feltárni racionális/szabályelvű keretrendszeren belül.”*[[13]](#footnote-13)

[3] A harmadik projektben, vagyis a ZH-javítókulcsok feltörésében már a kódolás nem is értelmezhető direkt módon, ellenben a social engineering[[14]](#footnote-14) (vagyis a pszichológiai manipuláció) egy speciális esete kerül bemutatásra, ahol is a tanári visszaélések ellen védekezni akaró diákok önszerveződése (saját megoldások archiválása és közös rendszerbe való feltöltése – „kódtörő-szakszervezet”) és némi matematika (vö. Solver-alapú optimalizálás) segítségével a tanári önkény és a javítókulcs (mint egy fajta kód) „megtörhető”[[15]](#footnote-15). Az innováció itt kevésbé matematikai, mint az ember-ember-kapcsolati rendszerek újragondolására alapuló, bár számos érdekes matematikai kérdés is felvetődik: pl. mennyi és milyen minőségi alapadat esetén milyen biztonsággal várható a kódok sikeres feltörése? Ez a gondolatvilág pedig már visszacsatol a konzisztencia fogalmához, ami a MI egyik legnagyobb, ha nem a legnagyobb gyengesége (vö. Jóság-fogalom komplexitásának alacsony szintje, sőt ennek teljes hiánya)…

# Alapvetések és benchmarkok

Kvázi minden kriptográfiai oktatás a Caesar-kóddal és annak feltörésével kezdődik, ahol a szekvenciális, korlátozott méretű ábécét körré alakítják, hogy egész számot használhassanak kulcsként a kódoláshoz / dekódoláshoz. Ezzel párhuzamosan egy pixel-alapú logika egyfajta "digitális/bináris kódolásként" értelmezhető, és ezek a kifejezések számos[[16]](#footnote-16) publikációban régóta beazonosíthatók.

A bináris kódolás fogalmára vonatkozó asszociációs tér lehetővé teszi tetszőleges objektumok bináris jellemzőinek elemzését. Ami a betűket/számokat illeti, a bináris változat egyfajta pontmátrix. Másrészt a fekete-fehér képek bináris alapinformációk alapján is értelmezhetők. Ha a bináris értékek értelmezési terét megadjuk, akkor alapvetően egész számokat definiálunk (lásd a 0-255 közötti pixelek szürkeárnyalatos értékeit) ugyanazokra a "változókra" (pixel-pozíciókra). A Caesar-kód és a betűk/számok (karakterek) digitalizálása lehetővé teszi, hogy a de/kódolási folyamatok fókuszát karakterről pixelre változtassuk.

A bináris pixel-értékek potenciális/kreatív transzformációinak területén a következő asszociáció a genetikus algoritmusok fogalma lehet, ahol a megoldás ábrázolásához szükséges bináris értékek úm. rafinált/szokatlan módokon megváltoztathatók (vö. mutáció, keresztezés)[[17]](#footnote-17).

És végül, a kép és/vagy a pontmátrix pixelei egy 2D-s (ill. igény esetén 3D-s, több dimenziós) kapcsolatokkal rendelkező rendszer celláiként is értelmezhetők. Ez vezet el a celluláris automaták fogalmához, ahol a bináris pixelek, mint sejtes információk többé-kevésbé egyszerű szabályok alapján megváltoztathatók.[[18]](#footnote-18)

Summa summarum: immár a pixel-alapú rejtjel-LEGO-játék minden összetevője adott. A következő fejezet a már lezárt kísérleteket mutatja be a valós lehetőségek és a valódi korlátok érzékeltetésére:

# Eredmények: szcenáriók/verziók

1. Bináris Caesar-kód egy betűre vonatkozó pixel-mátrixból képzett körkörös mintázat alapján[[19]](#footnote-19):
	1. Jól ismert nyomtatott betűtípusok (vö. munkalap: letter-univers3 és letter-universe2): a körkörös mintázat-építésnek kvázi korlátlan lehetőségi tere vélelmezhető különböző kockázatokkal és számítási igényekkel (lásd az 1. ábra): pl. sor-orientált, oszlop-orientált, minta-orientált, ill. először a páros, majd a páratlan pozíció-sorszámok vagy fordítva, vagy maradékos osztással, ahol az osztó nem a körelemszám maradéknélküli osztója) stb. Az ugyanazon a transzformációs logikán alapuló kódolás újra és újra megismételhető (lásd az 1. ábra – pl. az alsó rész) – az ismétlési érték származtatható például PI-ből vagy akár ismert sorozatokból (vö. Fibonacci, ahol mindig az utolsó betű -pozíció értékét el kell fogadni – ez azt jelenti, hogy mindössze 10 ismétlés kell a 0-9 közötti értelmezési intervallumban.
	2. Kézzel írt karakterek esetén nem feltétlenül releváns a méretezett/normalizált betűtípus. Valódi kézzel írott szövegek (ahol akár a szerzők eredetisége párhuzamosan ellenőrizhető is) n\*m pontmátrixra szeletelhetők, amely alapadatok az 1a-hoz hasonlóan ismét csak átalakíthatók. A kódolt üzenetek szegélyei tetszőleges helyeken húzhatók meg, mely szeletelési paraméterek maguk is a titkosítási eljárás részei. Ezért ez a fajta szeletelés a zavarkeltő hatások további rétege. A betűknek lehetnek különböző méretű pont-mátrixai is, ahol a pont-mátrix típusai PI-vel vagy más sorozatokkal szabályozhatók (például Fibonacci - pl. az utolsó (két) karakterpozíció a sor- és az oszlop-koordináta).





Ábra#1: Egyszerű (fent) és komplex (lent) körkörös minta-képzés egy betű egy objektum elven (forrás: cryprt1.xlsx)

1. Kettő vagy több digitalizált karakterhely egy képobjektum részeként közös pont-mátrixként értelmezve
	1. Nem szükséges új ábrákat (mint például #1) bemutatni az 1a és 1b szcenáriók alapján annak érzékeltetéséhez, hogy a pont-mátrixok tetszőlegesen kicsik vagy nagyok lehetnek egy ún. szabványos mérettől eltérően. Nem csak egy karaktert, hanem tetszőleges karaktereket is lehet kódolni (transzformálni) egy transzformáción belül, ahol az eredeti objektum (pont-mátrix) tetszőleges betűket/számokat ír le (vö. kézírás, mint opció – ill. pl. kínai írásjelek). Értelemszerűen a párhuzamosan kódolt betűk/számok dekódolása is párhuzamosan történik.
	2. A közös/blokkosított pont-mátrixok építésére nem az egyetlen út a betűhelyek összevonása: ugyanis egy holisztikus kép (pl. kézzel írott levél) tetszőleges módon szeletelhető (pl. Tetris-jellegű minták, sorozat-alapú minták).
2. Celluláris (sejtes) automaták:
	1. Dekódolható transzformációk: A pont-mátrixokra értelmezett bináris Caesar-kód, mint olyan, celluláris automatára vonatkozó szabályként is értelmezhető. A szabály egyszerű: egy cella új értéke legyen a szomszédos cella értéke. Fontos kiemelni, hogy a szabály egyetlen szomszédos cella esetén (vö. körkörös mintázat) triviálisan dekódolható.
	2. Nem dekódolható transzformációk: Egynél több érintett (szomszédos) cellát tartalmazó szabály esetén nem triviális, hogy a dekompozíció/dekódolás egzakt módon végrehajtható. Például: egy cella új értéke 1 legyen, ha a szomszédos (pl. 8) cellákban lévő értékek összege páros, a cella új értéke pedig nulla, ha az összeg (a fent leírtak szerint épül fel) páratlan szám. (Ugyanez a logika érvényes pl. a modulo-orientált szabályokra). A bináris kimeneti értékek (1;0) több, mint 2 bemeneti esetből (2^8) származnak, ezért nem triviális egy kimeneti értékből visszavezetni, melyik bemeneti kombináció állt mögötte. Azonban mégis lehetőség van dekódolható szabályok létrehozására egynél több, egy szabályban szereplő bemeneti cella alapján is: ha elkerüljük a bináris kimeneteket (lásd: cellaautomata3 – 2. ábra). Nem dekódolható transzformáció minden olyan transzformáció, ahol a bemeneti értékeknek egynél több kimeneti helyettesítője van (lásd a cellaautomata1&2 lapokat – 3. ábra). Kvázi korlátlan számú nem dekódolható transzformáció definiálható, például a fókuszált (szomszédos) cellák bináris tartalma különböző szekvenciákat építhet 0-ból és 1-ből, mint egy klasszikus bináris szám, és ezek a bináris módon leírt számok átalakíthatók 1-re vagy 0-ra jellemzőiktől függően (mint például a hexa-kódban vannak számok vagy sem)…



Ábra#2: Dekódolható celluláris automata – szabály = sum(oszlop)+3\*saját-érték (forrás: crypt1.xlsx)





Ábra#3: Output-szintű antagonizmusok (forrás: crypt1.xlsx) – Jelmagyarázat: a felső állapot szabálya = = sum(oszlop)+saját-érték, az alsó állapot szabálya = sum(oszlop)-saját-érték, bekeretezett cellák = antagonizmusok

1. Genetikus algoritmus-jellegű transzformációk
	1. Mutációk helyett: minden bemeneti sejtmintát meg kell fordítani, ahol egy sejtminta lehet egy 2\*2-es sejtobjektum (lásd #4. ábra – munkalap: mutáció). Itt és most immár triviálisnak kellene lennie, hogy minden transzformációs típushelyzet egy fajta mutáció (vö. sejtautomata, körkörös mintázat, stb.), vagyis teljesen lényegtelen a címkézés, mint olyan – hiszen csak transzformációs szabályok vannak (dekódolható vagy nem dekódolható formában).
	2. Keresztezés helyett: a 2\*2-es mintát keresztezésnek is nevezhetnénk (a 2\*2-es mintán belül), de az 5. ábra részben (felső) és teljes (alul) keresztezési mintákat mutat be (lásd munkalap: crossing):



Ábra#4: 2\*2-mintázat: mutáció (forrás: crypt1.xlsx)



Ábra#5: Részleges/teljes keresztezések (forrás: crypt1.xlsx) – Jelmagyarázat: felső részleges mintázat: 4\*4-es blokk transzponálva középen, alsó mintázat: 4(4\*4) blokk transzponálva saját helyükön (forrás: crypt1.xlsx)

1. Pixel-alapú karakterek dekompozíciós kódolása
	1. Véletlenszerű dekompozíció: A 6. ábra egy olyan dekompozíciós példát mutat be, ahol 3 randomizált réteget integrálunk a végső képbe. A véletlenszerű effektusok nagyon alacsony gyakorisággal vezetnek hasznos üzenetekhez (lásd a 4. képelem – középen a felső részen).
	2. Optimalizált dekompozíció: Ha a bemenet (az ún. 4. képelem előre meghatározott, akkor a dekompozíció véletlenszerű értékekkel is végrehajtható: az első érték a teljes értelmezési térben generálható, a második érték értelmezési tére az első véletlen értékkel csökkentett érték, az utolsó érték pedig egyfajta maradék (lásd a 6. ábra alsó részét egy kontroll képpel középen) Az értelmezési tér szürkeárnyalatos intervallumokra (0-255) optimalizálható. A dekompozíció keretében előállt rétegek bármikor, bármilyen nyilvános módon kommunikálhatók a címzettek felé ún. soha nem-dekódolható üzenetként. Hiszen a kódtörők soha nem fogják tudni a dekompozíciós rétegek egyike alapján: hány további réteg szükséges még a végső képhez, és hogyan kell integrálni az egyedi dekompozíciós rétegeket.



Ábra#6: Véletlenszerű és optimalizált dekompozíciós rétegek és eredőjük (forrás: crypt1.xlsx) – Jelmagyarázat: fent = véletlenszerű, alul = optimalizált rétegek és ezek eredője

Egy fajta titkos-kulcs-jellegű megközelítés lehet az, ha egy vagy több dekompozíciós réteget már megadnak a fogadók számára eleve előre a kódolási szabályok részeként, és a küldők is ismerik ezeket a rétegeket természetesen, így a küldők bevonhatják ezeket a dekompozíciós folyamatok optimalizálásba. Az elküldött rétegek száma ezáltal lecsökkenthető, ami azt jelenti, hogy a kódtörő soha nem fogja látni az üzenet összes komponenst, hiszen az előre egyeztetett rétegek nem kerülnek soha többé kommunikálásra a feltörők által megfigyelhető csatornákon.

# Vita

A karakter-(betű/számjegy)-alapú kódolás kevesebb erőforrást igényel, mint pixel-alapú átalakítási megközelítés. Ezért az itt és most bemutatott megoldásokat olyan esetekben érdemes alkalmazni, amikor a rövid üzeneteket és/vagy fontos képeket minőségi/ritka/egyedi módon kell védeni.

A fent említett megoldás-variánsok többnyire kombinálhatók egymással. Ezért a kombinatorikai tér kvázi korlátlanul növelhető a számítási idő terhére.

Az itt és most (részletesen) ki nem fejtett karakterisztikák esetleges hiánya a potenciális kódolási technikák gyengeségeként is értelmezhetők: vö. a betűgyakoriság kiegyenlítés: további, jelentés nélküli eredeti szövegrészek által, vagy az eredeti szöveg áttervezésével pl. ismétlődő betűkkel elért statisztikák révén, ahol az ismétlések nem zavarják az értelmezéseket (pl. ggyyakoriissáág).

Emellett az eredeti betűk/számok nem csak egyetlen (saját) pont-mátrixok keresztül ábrázolhatók, hanem akár átfedésekkel is.

# Konklúziók

Az effajta alapötletek ritkasága/egyedisége és a technika ab-ovo ritka alkalmazása kvázi lehetetlenné teszi az ilyen típusú kódok ad hoc jellegű felmerülése esetén ezek feltörését.

Az érintett személyek/rendszerek közötti felkészülési szakasz nem csökkenthető nullára. A kódolási stratégiák alaplogikáit meg kell osztaniuk egymással a küldő és fogadó feleknek mindenképpen előre.

# Jövőkép

A nem dekódolható transzformációknak lehet olyan részhalmaza, ahol a kódolási szabályokat ugyan nem lehet megfordítani a dekódolás érdekében, de lehetségesnek tűnik pl. Solver-alapú dekódoló megoldások levezetése, mint például a javítókulcs-feltörések (ill. aknakereső játékok) esetében. Cél: a jövőben legalább egy bemutató verziót feltárni...

Az itt bemutatott innovációk ezen megoldások kriptográfiai piaci értékétől függetlenül azon oktatási folyamatokhoz szervesen és hasznosan kapcsolhatók, ahol az informatikai biztonság iránt érdeklődő hallgatók szeretnék megtanulni forráskódok létrehozását mátrix-függő problémák esetén.

# Irodalomjegyzék

Pitlik, L. el al (2023): Demo materials for a pixel-based cryptography, MIAU-Journal, No.303, <https://miau.my-x.hu/miau/303/crypt1.xlsx>

Pitlik, L. et al (2022): Derivation of evaluation test-codes based on solver in different case, MIAU-Journal, No.282-283, <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=jav%C3%ADt%C3%B3kulcs>

Pitlik, L. et al (2021): Robot-aesthetic-expert or the mathematics of the beauty - Part, MIAU-Journal, No.270, <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=aesthetic>

Pitlik, L. et al (2019): Cipher - exercises for advanced users – Part I-II-III, MIAU-Journal, No.254, <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=cipher>

Pitlik, L. et al (2018): Genetic algorithms for problem solving - reproducible demo, MIAU-Journal, No.244, <https://miau.my-x.hu/miau/244/ga_excel.xlsx>

Pitlik, L. et al (2018): Simple cellular automata based on Excel-makros, MIAU-Journal, No.237, <http://miau.my-x.hu/miau/237/cellu1.xlsm>

Márton, Gy. (2023): Cryptography, Sapientia University, <https://www.ms.sapientia.ro/~mgyongyi/Crypto/Labor1.html>

Buttyán, L. et al (2006): Kódolástechnika, BME, <https://www.hit.bme.hu/~buttyan/publications/bscinfkod.pdf>

# Mellékletek

Forrás: <https://miau.my-x.hu/miau/303/crypt2.xlsx>





Ábra#7: Letter-ASCII-Binary-Shifting-ASCII-Letter-módszer (forrás: crypt2.xlsx)

A betű-alapú (LABSAL) megközelítés a 7. ábrán bemutatott módszertanon keresztül finomhangolható. Az átalakítási szabályok bonyolultabbak, mint a régi Caesar-kód esetében. Ugyanaz a betű a sima/eredeti szövegben nem mindig ugyanaz az eltolt transzformációk után, vagyis nem lehetetlen az azonosság (lásd fent a 7. ábrán a szóközöket). A LABSAL-megközelítés kevesebb erőforrást igényel, de ugyanazok a kockázatok itt is fellépnek, mint a betűből betűt képző kódok esetén…

\*\*\*

Transzkripció-alapú kriptográfia egy, a TEAMS véletlenszerűen fellépett átírási funkciójából fakadó ötlet, ahol a magyar beszélő hangját egy fajta angol robotfülön keresztül írják át a háttéralgoritmusok angolnak remélt szöveggé. A kimeneti szöveg egy teljesen új nyelvnek tűnik azonban, amelyet egy MI automatikusan hozott létre (vö. kódolási automatizmus). A jövő kérdése már csak az, hogy ezek a kimeneti szövegek dekódolhatók-e triviális (inverz) szabályok és/vagy tanulási minták alapján? Demo: <https://miau.my-x.hu/miau/300/transcription-based-cryptography.mp4>

\*\*\*

A Rohonczi kódex (<https://hu.wikipedia.org/wiki/Rohonci_k%C3%B3dex>) említése azért érdekes ezen a helyen, mert a pixel-betű-szó(tag)-nyelv tengely így válik teljessé: A betű-alapú kódoláshoz képes a cikkben bemutatott pixel-alapúság a skála egyik irányába mozdul el, míg a mesterséges nyelv kialakítása a másik irányba (<https://www.youtube.com/watch?v=oxjqsTwRUbc&t=283s>). A szó(tag)-írás (vö. kana), hieroglifák (vö. <https://hu.wikipedia.org/wiki/K%C3%ADnai_%C3%ADr%C3%A1s>) furcsa módon inkább kódolható pixel-grafikusan (kivéve, ha előtte átírásra kerül a szöveg betűírásra (pl. <https://translate.google.com/?hl=hu&sl=zh-CN&tl=hu&text=%E8%B0%A2%E8%B0%A2&op=translate> - 谢谢 -Xièxiè), mint új nyelv feltalálásával (amivel természetesen bármi kódolható elvileg).

\*\*\*

A titkosírások kapcsán alapvető kérdés: rá lehet-e jönni egy adott kódrészlet alapján arra, vajon véletlenszámgenerátoros „megoldásról” (átverésről) van-e szó, vagy sem. Ennek a kérdéskörnek egy speciális esete az a modern kihívás, amikor pl. a chatGPT által írt (kódolatlan szövegek kapcsán) azt kell felismerni, hogy ezt a chatGPT írta-e?! (vö. Turing-teszt)…

1. <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=cipher>,

<https://miau.my-x.hu/miau2009/index.php3?x=e0&string=aesthetic>,

<https://miau.my-x.hu/miau2009/index.php3?x=e0&string=jav%C3%ADt%C3%B3kulcs> [↑](#footnote-ref-1)
2. <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=cipher>,

<https://miau.my-x.hu/miau2009/index.php3?x=e0&string=aesthetic>,

<https://miau.my-x.hu/miau2009/index.php3?x=e0&string=jav%C3%ADt%C3%B3kulcs> [↑](#footnote-ref-2)
3. <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=pixel-based.cryptography> [↑](#footnote-ref-3)
4. <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=cipher> [↑](#footnote-ref-4)
5. <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=aesthetic> [↑](#footnote-ref-5)
6. <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=jav%C3%ADt%C3%B3kulcs> [↑](#footnote-ref-6)
7. <https://miau.my-x.hu/miau/254/cipher1.docx> [↑](#footnote-ref-7)
8. [https://miau.my-x.hu/miau2009/index\_tki.php3?\_filterText0=\*knuth](https://miau.my-x.hu/miau2009/index_tki.php3?_filterText0=*knuth) [↑](#footnote-ref-8)
9. <https://miau.my-x.hu/miau/254/cipher2.docx>) [↑](#footnote-ref-9)
10. <https://miau.my-x.hu/miau/254/cipher3.docx> [↑](#footnote-ref-10)
11. <https://hu.wikipedia.org/wiki/Szteganogr%C3%A1fia> [↑](#footnote-ref-11)
12. <https://miau.my-x.hu/miau/270/roboteszteta.docx> [↑](#footnote-ref-12)
13. <https://miau.my-x.hu/miau/270/roboteszteta_II.docx> [↑](#footnote-ref-13)
14. [https://hu.wikipedia.org/wiki/Pszichol%C3%B3giai\_manipul%C3%A1ci%C3%B3\_(informatika)](https://hu.wikipedia.org/wiki/Pszichol%C3%B3giai_manipul%C3%A1ci%C3%B3_%28informatika%29) [↑](#footnote-ref-14)
15. <https://miau.my-x.hu/miau2009/index.php3?x=e0&string=jav%C3%ADt%C3%B3kulcs> [↑](#footnote-ref-15)
16. <https://www.ms.sapientia.ro/~mgyongyi/Crypto/Labor1.html>, <https://www.hit.bme.hu/~buttyan/publications/bscinfkod.pdf> [↑](#footnote-ref-16)
17. <https://miau.my-x.hu/miau/244/ga_excel.xlsx> [↑](#footnote-ref-17)
18. <http://miau.my-x.hu/miau/237/cellu1.xlsm> [↑](#footnote-ref-18)
19. <https://miau.my-x.hu/miau/303/crypt1.xlsx> [↑](#footnote-ref-19)