New Records for Playfair Solutions

Louie Helm (presenter) and Richard Bean

HistoCrypt 2025

Poznań

17 June 2025

Playfair Challenges Recap

- Klaus Schmeh blog ran Playfair cipher challenges (50 → 24 letters) from 2018-2020
- Dunin et al. (2022) proposed a tougher 22-letter challenge
- 24 and 22 below/near Deavours unicity distance (1977) (≈ 22.7 letters) → many plausible plaintexts

CRYPTOLOGIA
2022, VOL. 46, NO. 4, 302–322
https://doi.org/10.1080/01611194.2021.1905734

Taylor & Francis
Taylor & Francis Group

How we set new world records in breaking Playfair ciphertexts

Elonka Dunin, Magnus Ekhall, Konstantin Hamidullin, Nils Kopal, George Lasry, and Klaus Schmeh

Earlier Challenge Solutions*

- WHILE IN PARIS I RECEIVED ORDERS TO REPORT TO GENERAL FOSTER (50)
- MEET YOU TOMORROW AT FOUR TWENTY AT MARKET PLACE (40)
- TAKE THE LAST TRAIN TO YORK ON SUNDAY (30)
- STAY WHERE YOU ARE UNTIL THURSDAY (28)
- WAIT FOR FURTHER INSTRUCTIONS (26)

**posted on Klaus Schmeh's Cipherbrain blog (2018-2022); †see Dunin et al., "How we set new world records …" (2022)*

Cryptanalytic Workflow

- Letter n-gram tables 7-10-gram (8 GB → 90 GB RAM)
- With n=7, 26^7 = 8,031,810,176
- With n>7, not all n-gram scores stored – split e.g. n=8 with top 125,000 4-grams indexed
- Positional letter n-gram scoring for n=8, 9
- Word-split scoring with large language models (KenLM)
- Screened ≈ 4 B (24-ltr) & 1.8 B (22-ltr) candidates

Letter n-gram Models

- AZdecrypt 7–10-gram stats (Jarlve & Beijing House)
- Good for ≥26-letter texts; ineffective here
- Correct plaintext never ranked in top 50 000 by letter score alone

Language Model #1 – "books3"

- 200 k English books (100 GB) → 16 B unique 1-5-grams
- KenLM trie 163 GB; vocabulary 140 k (J→I mapping)
- Ranked 22-ltr answer in top 10 k; missed 24-ltr due to split bug

Language Model #2 – "CommonCrawl"

- A huge (6 TB) model from 2014
- 23 TiB crawl → 500 B unique 1-5-grams, unpruned
- 6 TB trie file, run from SSD; Kneser-Ney smoothing
- Ranked solutions: 22-ltr top 5 k, 24-ltr top 2 k

From Scores to Solutions

- Pipeline: 96-thread simulated annealing → Top candidates rescored with two LMs (books3, CommonCrawl)

- 22-letter challenge – phrases common to top lists of BOTH LMs:
  - WOULD EVERYONE CARE FOR IT
  - PILLARS OF THE INSANITY
  - AVOID VISUAL DEFICIENCY
  - THE VERDICT WOULD BE HALF

- 24-letter challenge – samples present in top-20 of BOTH LMs:
  - AFTER THAT ABOUT CLOSING UP
  - GIFTS BESTOWED TO HER FAMILY
  - IN EVOLVING THE WORLD MUSIC
  - ITS HUGE PERFORMANCE MAGIC
  - THEY SAY THE LIQUOR HAD GONE
  - WE ARE CREATING A BOLD PILOT

From Scores to Solutions

- books3's single highest-scoring lines:
  - WOULD EVERYONE CARE FOR IT (22) – strong margin
  - AND PERHAPS HES COLLECTING (24) – line 84 in trie list
  - WAIT COME BACK TO US FIRST (22) – lines #848 / #102

- Manual review favoured concise imperative sentences with a spycraft theme. Final solutions:
  - FIND DEAD DROPS BELOW BRIDGE (24)
  - MONEY IS HIDDEN BEHIND HUT (22)

What Made 24 & 22-letter Challenges So Hard?

- Plaintext of challenges didn't contain article or connector words
- Letter-level stats saturated by false positives
- N-gram letter scored output never saw true solution in top 50 k solutions
- Search space: $25! \approx 1.55 \times 10^{25}$ keys (J=I) → heuristic search essential

Key Takeaways

- Short Playfair texts defeat pure letter n-gram scoring
- Massive word-level LMs move intended solution well up the ranking
- Domain-specific corpora could help further
  - A “harmful” LM gave quite different solutions
- AI-generated text in modern corpora → future noise

Thanks & Q / A

- Method pushed Playfair solving to new limits
- https://github.com/doranchak/azdecrypt for n-gram stats and FreeBasic code for using special stats, n>7
- https://github.com/RichardBean/Playfair for 9-gram C code
- Contact: louiehelm@protonmail.ch r.bean1@uq.edu.au