Khoảng xác định duy nhất của mật mã Zodiac-340

TS. Trần Duy Lai

Zodiac-340 là một bản mã dựa trên các mã pháp cổ điển là thay thế và hoán vị, nhưng việc phá nó không hề dễ. Trong [1] cũng đã trích dẫn nhiều bài viết về lời giải của Zodiac-340. Trên trang web của Hiệp hội quốc tế về nghiên cứu mật mã, ngày 12/12/2021 đã xuất bản bài viết của Joachim von zur Gathen với nhan đề "Unicity distance of the Zodiac-340 cipher". Bài viết này sẽ trình bày lại kết quả của nghiên cứu này.

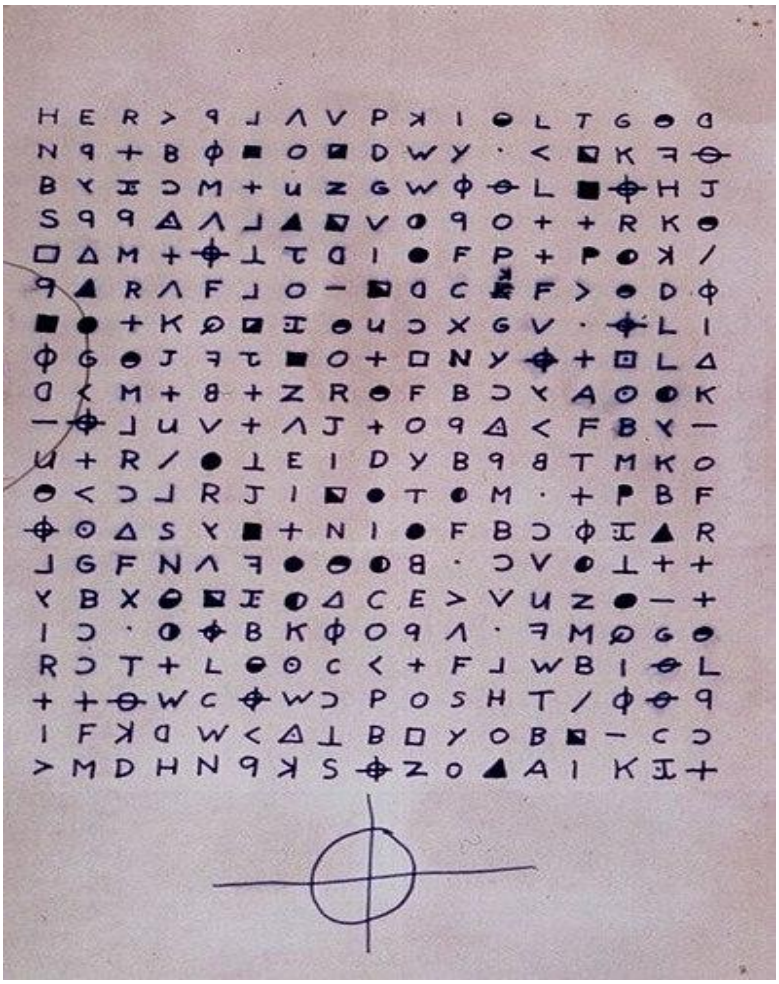
Mở đầu

Vào tháng 12/2020, David Oranchak, Jarl Van Eycke và Sam Blake đã giải được một bí ẩn 51 năm: mật mã Zodiac gồm 340 ký hiệu. Tính đúng đắn của lời giải đó không bị nghi ngờ và [2] đưa ra một lập luận có lợi cho nó: khoảng xác định duy nhất của hệ thống mật mã tối đa là 152.

Trong 2 năm 1968 và 1969, một kẻ sát nhân hàng loạt đã giết chết 5 người ở khu vực Vịnh San Francisco. Kẻ sát nhân đã khoe khoang về chiến công của mình trong những lá thư gửi cho Sở Cảnh sát và báo chí địa phương. Một số trong số chúng đã được mã hóa, một thư có 408 ký hiệu và một thư khác có 340 ký hiệu. Chúng được gọi lần lượt là Zodiac-408 và Zodiac-340. Một số bức thư khác cũng được mã hóa nhưng chúng quá ngắn để cho phép giải mã. Nhiều vụ giết người và các tin nhắn khác được cho là có liên quan đến Zodiac, nhưng chúng chưa được xác nhận. Bất chấp nhiều manh mối mà kẻ sát nhân cung cấp, tên tội phạm chưa bao giờ bị phát hiện.

Zodiac-408 sử dụng phép thế đa biểu và đã được giải trong vòng một tuần bởi thầy giáo Donald Harden và vợ ông là Bettye. Nhưng Zodiac-340, bức thư được gửi trên một tấm bưu thiếp vào ngày 08/11/1969, vẫn là một thách thức lớn đối với những người phá mã. Nhiều người đã bị thu hút bởi thử thách này. Một số lời giải cũng đã được đề xuất, nhưng không có lời giải nào thuyết phục được đa số các chuyên gia. Một câu hỏi đặt ra là: để tìm ra lời giải cho mật mã này có cần đến các kiến thức toán học phức tạp của mật mã hiện đại cũng như sức mạnh tính toán của các siêu máy tính?

Vào tháng 3/2013, David Oranchak - kỹ sư phần mềm người Mỹ đã lập ra trang web zodiackiller[.]net, nơi tổ chức các nỗ lực để giải Zodiac-340 một cách có hệ thống, kết hợp cả tài khéo léo của con người và năng lực tính toán, với các quan sát của những người quan tâm và các dự án phần mềm. Dự án tính toán và tư duy cộng đồng này đã thành công vào ngày 11/12/2020 khi Oranchak cùng với nhà toán học người Úc Sam Blake và nhà lập trình người Bỉ Jarl Van Eycke, tuyên bố phá vỡ mật mã.



Hình 1. Bản mã Zodiac-340

Tính đúng đắn của lời giải của họ chưa có thách thức đáng kể và đã được FBI xác nhận công khai. Công trình [2] cho thấy rằng lý thuyết của Shannon về khoảng xác định duy nhất trong giải mã ủng hộ lời giải này.

Khoảng xác định duy nhất

Trong số nhiều lời giải của Zodiac-340 đã được đề xuất, lời giải nào là "tốt hơn" hay "đúng"? Mỗi người sẽ có những ý kiến khác nhau, đặc biệt là những người đã đề xuất ra lời giải.

Nhưng có một câu trả lời khoa học cho câu hỏi này dựa trên lý thuyết của Shannon về khoảng xác định duy nhất. Nó yêu cầu mô tả của hệ mật sử dụng khóa bí mật và một khóa cụ thể được sử dụng. Lý thuyết dẫn đến một giá trị nhất định, được gọi là khoảng xác định duy nhất (unicity distance), mà kết quả giải mã của một bản mã dài hơn giá trị này với xác suất cao là duy nhất và theo lý thuyết này được chấp nhận là đúng.

Nhà toán học, kỹ sư điện và mật mã người Mỹ Claude Elwood Shannon (1916-2001) đã đưa ra nền tảng lý thuyết thông tin của truyền tin và mật mã. Ông đã định nghĩa các khái niệm về entropy thông tin và nội dung thông tin trên các không gian xác suất. Chúng ta quan tâm đến khái niệm của ông về khoảng xác định duy nhất *d*:

$$d = I(\text{khóa})/[\log_2(\text{độ\_dài}) - H(\text{ngôn\_ngữ})]. \qquad (*)$$

Điều này áp dụng cho việc giải mã một bản mã có *độ_dài* bit, được mã hóa trong hệ mật với các khóa có nội dung thông tin *I(khóa)* bit, trong đó các bản rõ đến từ một ngôn ngữ có entropy bằng *H(ngôn_ngữ)* và $\log_2$ là logarit theo cơ số 2. Định

lý nổi tiếng của Shannon khẳng định rằng khi bản mã có nhiều hơn *d* ký hiệu, thì việc giải mã được mong đợi là duy nhất.

Trong [2] đã ước lượng khoảng xác định duy nhất (*) của một mã pháp mà đã tạo ra Zodiac-340, đó là sự kết hợp của 4 thành phần sau:

- Một phép thế đa biểu được chọn ngẫu nhiên của 26 chữ cái biến thành 63 ký hiệu;
- Phép chia bản mã thành tối đa 3 phân đoạn ngang hoặc dọc;
- Phép chuyển vị cho tới 51 vị trí;
- Một số thay đổi bất quy tắc ở các chữ cái riêng lẻ.

Các phép thế đa biểu

Entropy của các lựa chọn ngẫu nhiên đóng một vai trò trung tâm trong lý thuyết của Shannon. Phiên bản đơn giản nhất của nó đề cập đến một không gian xác suất hữu hạn A có các phần tử a được gắn kèm xác suất xảy ra không âm p_a. Có một điều kiện là $\Sigma_{a\in A}\, p_a = 1$. Khi đó entropy là

$$H = -\sum_{a\in A} p_a \log_2(p_a).$$

Dấu '–' là do đại lượng $\log_2(p_a)$ là số không bao giờ dương. Độ đo này thích hợp trong một số trường hợp, ví dụ, đối với việc lựa chọn ngẫu nhiên đều của các khóa trong số S khả năng. Khi đó $p_a = 1/S$ cho tất cả các khóa a, mỗi số hạng trong tổng ở trên bằng $1/S \cdot \log_2 1/S) = -\log_2(S)/S$. Có S số hạng và $H = \log_2(S)$.

Đối với phép thế đa biểu, nói chung có hai tập hữu hạn (bảng chữ cái): X gồm m chữ cái bản rõ, Y gồm n ký hiệu bản mã và mối liên kết giữa mỗi chữ cái bản rõ với một số ký hiệu bản mã, cũng có thể không có. Về mặt toán học, đó không phải là một hàm từ X vào Y, mà là một hàm f: $Y \rightarrow X$. Hàm f này tương ứng với bước giải mã, mà kết quả của nó được giả định là duy nhất.

Số của tất cả các hàm f như vậy là m^n. Trong trường hợp của Zodiac-340, $m = 26$ và $n = 63$ (Hình 1). Do đó, không gian khóa cho các phép thế đa biểu này bao gồm chính xác 26^{63} phần tử và nội dung thông tin của một khóa được chọn ngẫu nhiên đều là

$$I(\text{các phép thế}) = \log_2(26^{63}) \approx 196.13.$$

Bản mã được phân đoạn

Mật mã bao gồm 20 hàng, mỗi hàng có 17 ký hiệu. Trong quá trình nghiên cứu, những người phá vỡ Zodiac đã nghi ngờ (một cách chính xác) rằng bản rõ có thể đã được chia thành nhiều phần. Họ đã thử từ 1 đến 3 phân đoạn theo chiều ngang,

mỗi phân đoạn bao gồm các hàng ngang liền nhau trong số 20 hàng trong bản mã và tương tự đối với các phân đoạn theo cột dọc của 17 cột.

Nếu các phân đoạn nằm ngang chứa r_1, r_2, r_3 các hàng liền kề, với các giá trị không âm r_i và $r_1 + r_2 + r_3 = 20$, thì các số này tạo thành một sự kết hợp của 20 số thành nhiều nhất là 3 phần. Số cách ghép của l phần tử thành đúng i phần là $\binom{l-1}{i-1}$, và do đó số các khả năng cho các phân đoạn theo chiều ngang và dọc là

$$\left[\sum_{1\le i\le 3}\binom{19}{i-1}\right]\cdot\left[\sum_{1\le i\le 3}\binom{16}{i-1}\right] = 191\times 137 = 26167.$$

Do vậy, đóng góp entropy của việc phân đoạn là

$$I(\text{phân đoạn}) = \log_2(26167) \approx 14.68.$$

Các chuyển vị

Phép chuyển vị là một biến đổi cổ điển trong mật mã. Bản rõ được trình bày dưới dạng chuỗi $x_0, x_1, x_2, \ldots, x_{l-1}$ của l ký hiệu và độ dài chuyển vị t (chính xác hơn, phép chuyển vị ở đây được hình thành trên cơ sở phép lấy cách đều theo t) được chọn. Bắt đầu với $y_0 = x_0$, mọi chữ cái thứ t của x xuất hiện trong văn bản chuyển vị y:

$$(y_0, y_1, y_2, .., y_{l-1}) = (x_0, x_t, x_{2t}, .., x_{(l-1)t}),$$

trong đó các chỉ số của x được lấy theo modulo l. Nếu l và t nguyên tố cùng nhau, thì khi chạy từ 0 đến (l -1) thì $j \equiv (i \cdot t) \bmod l$ sẽ là một hoán vị của (0, 1, … , l-1). Trong bước giải mã, y_j được cho và i được xác định bằng $i \equiv jt^{-1} \bmod l$, trong đó t^{-1} là nghịch đảo mô đun của t modulo l. Ở đây có một ẩn ý là sau phần tử cuối cùng sẽ đến phần tử đầu tiên. Chuỗi số không phải là một đoạn thẳng mà được coi như một vòng tròn mà hai đầu của đoạn được dán vào nhau.

Ví dụ với $l = 9\cdot 17 = 153$ và $t = 19$, chuỗi chỉ số bắt đầu bằng

0 1 2 3 4 5 6 7 8 9 . . . cho x,

0 19 38 57 76 95 114 133 152 171 ≡ 18 . . . cho y

nên chuyển vị của $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, \ldots$ là

$$y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, \ldots$$
$$= x_0, x_{19}, x_{38}, x_{57}, x_{76}, x_{95}, x_{114}, x_{133}, x_{152}, x_{18}, \ldots$$

Ta có $-8\cdot 19 = -152 = -153 + 1 \equiv 1 \bmod 153$ và vì thế $t^{-1} = 19^{-1} \equiv -8 \equiv 145 \bmod 153$. Có $18 \equiv 9\cdot 19 \bmod 153$ và $9 \equiv 18\cdot 145 \bmod 153$.

Ở trên, bản rõ được đưa ra dưới dạng một chuỗi trong định dạng một chiều. Mật mã Zodiac-340 sử dụng một biến thể hai chiều của nó. Hình 2 cho thấy biến thể 2 chiều đó được áp dụng vào 9 (trong số 20) hàng trên cùng. Đánh số các hàng là 0, 1,…, 8 và các cột là 0, 1,…, 16 trong bản mã Zodiac-340. Phần tử thứ hai ở trên nói rằng $y_1 = x_{19}$ và có thể được nhìn thấy trong ô màu vàng ở hàng thứ hai và cột thứ ba. Tương tự, $y_8 = x_{152}$ được hiển thị bằng con số 8 (màu xanh lục-vàng) ở góc dưới bên phải. Ô đó mang chỉ số lớn nhất, cụ thể là 152.

Vì chiều dài chuyển vị 19 lớn hơn chiều rộng 17 của hình chữ nhật 2 đơn vị, nên việc cộng thêm 19 tương ứng với chuyển 2 bước sang phải và 1 bước xuống dưới. Đây chính là phép '1,2-decimation' được nói tới trong [1].

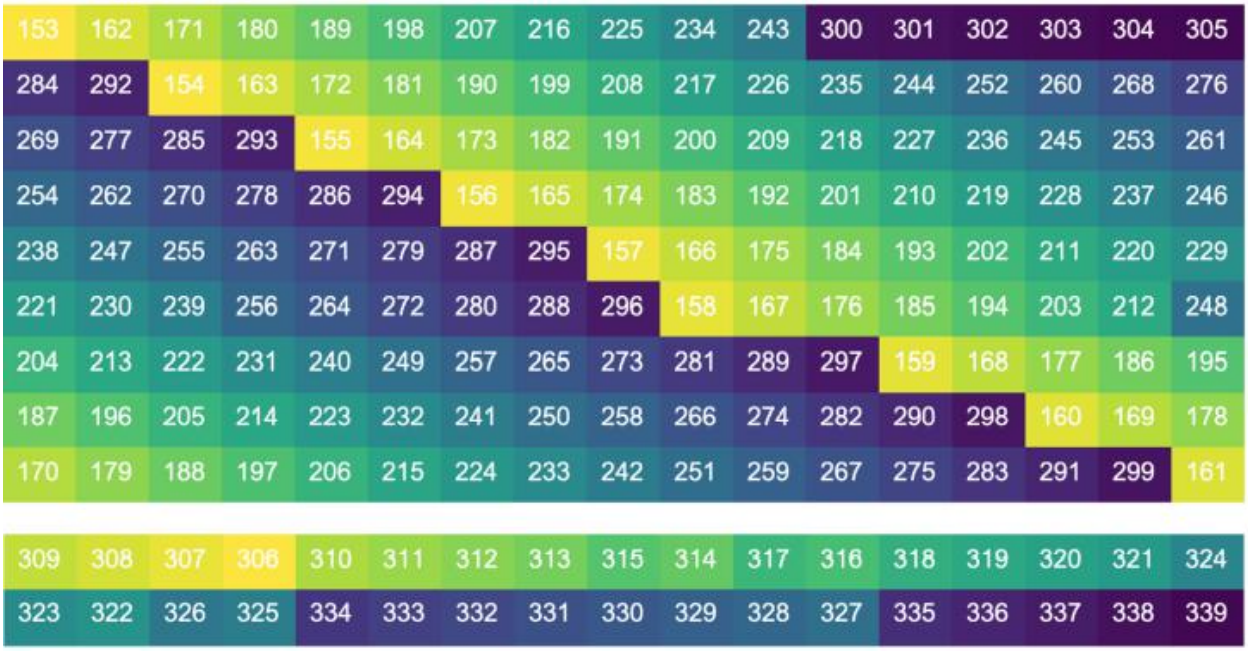
0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144
136	145	1	10	19	28	37	46	55	64	73	82	91	100	109	118	127
119	128	137	146	2	11	20	29	38	47	56	65	74	83	92	101	110
102	111	120	129	138	147	3	12	21	30	39	48	57	66	75	84	93
85	94	103	112	121	130	139	148	4	13	22	31	40	49	58	67	76
68	77	86	95	104	113	122	131	140	149	5	14	23	32	41	50	59
51	60	69	78	87	96	105	114	123	132	141	150	6	15	24	33	42
34	43	52	61	70	79	88	97	106	115	124	133	142	151	7	16	25
17	26	35	44	53	62	71	80	89	98	107	116	125	134	143	152	8

Hình 2. Chín dòng phía trên của Zodiac-340 được chuyển vị

Đến sau phần tử cuối cùng là phần tử đầu tiên. Vì vậy, hình chữ nhật biến thành một chiếc bánh rán, nơi các cạnh bên trái và bên phải cũng như trên và dưới được dán lại với nhau. Từ vị trí của ô có số 8, nước đi 2 bước sang bên phải và 1 bước xuống dưới đưa chúng ta tới ô có số 9.

Điều này xảy ra một cách có hệ thống. Ở cạnh bên phải, bước di chuyển mà chúng ta quan tâm đưa chúng ta 2 bước sang phải, ở hàng tiếp theo, rồi 1 bước đi xuống. Nhưng bước đi xuống không được thực hiện, thay vào đó chỉ là bước đi 2-0. Điều này tránh để lại một hàng không được sử dụng và chúng ta gọi quy trình này là không có hàng không được sử dụng (no unused rows).

Toàn bộ văn bản được chia thành ba hình chữ nhật nằm ngang, tất cả có 17 cột và tương ứng 9, 9 và 2 hàng. Các hình chữ nhật ở giữa và dưới cùng được thể hiện trong Hình 3.



Hình 3. Các phân đoạn giữa và dưới của Zodiac-340 được chuyển vị

Phần dưới cùng có hai hàng không liên quan đến bất kỳ sự chuyển vị nào. Trong số chín từ của nó, ba từ được viết đúng chính tả (các con số tăng dần) và sáu từ được viết ngược (các con số giảm dần). Việc đảo ngược các từ không tạo ra vấn đề lớn đối với việc giải mã và do đó không đóng góp nhiều vào việc bảo mật. Chúng ta bỏ qua nó trong phần sau ngoại trừ việc chúng ta cấp một bit cho việc có "sử dụng đảo ngược từ" hay không.

Bây giờ, độ dài chuyển vị tùy ý chạy từ 0 (không có chuyển vị) đến 51 và lựa chọn hai bit cho việc có hay không có hàng không được sử dụng và có đảo ngược từ hay không. Điều này cho tổng số $52 \cdot 2 \cdot 2 = 208$ khả năng và đóng góp vào I(khóa):

$$I(\text{chuyển vị}) = \log_2(208) \approx 7.70.$$

Các phép thế bất quy tắc

Một số khía cạnh của mật mã Zodiac-340 không nằm trong quy luật đã được xem xét ở trên của phép thế đa biểu, phân đoạn và chuyển vị. Đó là:

Lỗi chính tả

- Năm từ bị sai chính tả: FAN, BRINGO, BECAASE, SOOHER, E đáng lẽ là FUN, BRINGS, BECAUSE, SOONER, I.
- Phép thế Zodiac-340 không có ký hiệu bản mã cho K, và hai lần xuất hiện của chữ K lại được viết là V: WORV, VNOW lẽ ra là WORK, KNOW.

- PARADICE không chuẩn xác (phải là PARADISE) đã xuất hiện ba lần trong Zodiac-340 (nó cũng xuất hiện trong Zodiac-408) (trong đó có 1 lỗi đánh máy thành PARADLCE).

Ký tự giả

Các từ LIFE IS ở hàng áp chót của văn bản là các ký tự giả, có thể phục vụ để làm cho văn bản khớp chính xác với mảng hình chữ nhật của nó.

Bỏ qua

Trong hàng 15 (hàng thứ sáu của phần giữa), một chữ cái được chuyển từ vị trí thích hợp của nó ở cột thứ tư đến cột cuối cùng trong cùng một hàng. Đây là ô có nhãn 248 trong Hình 3.

Tất cả những điều bất quy tắc trên có thể được mô tả bằng cách cho phép vật thay thế (replacement) trong mã hóa (replacement là 'vật thay thế'/'vật được thay thế'; còn 'substitution' là 'hành động thay thế'). Cần giả định rằng bảng chữ cái tiếng Anh 26 chữ cái có thêm một chữ cái nữa, đó là khoảng trống ⋆. Nhưng đây không phải là một trống bình thường, mà là một ký tự vô hình. Do đó BRINGO và BRIN⋆GO được coi là như nhau. Thay đổi một chữ cái bằng ⋆ có nghĩa là loại bỏ chữ cái đó. Trong [2] đã tính có cả thảy 21 vật thay thế. Như vậy chúng ta có tổng cộng 21 vật thay thế trong văn bản 340 ký tự, nó khoảng 6.18%. Nếu chúng ta cho phép một cách rộng rãi 25 vật thay thế, thế thì có $R = \binom{340}{25} \cdot 27^{25}$ khả năng, với đóng góp vào I(khóa) bằng

$$I(\text{đánh đổi}) = \log_2(R) \approx 244.12.$$

Entropy của khóa và độ dài văn bản

Bây giờ đã sẵn sàng để xác định giá trị của I(khóa). Một khóa bao gồm 4 thành phần, mỗi thành phần được chọn một cách ngẫu nhiên đều và độc lập. Các giá trị được làm tròn là:

Phép thế đa biểu**:** $I(\text{phép thế}) = \log_2(2663) \approx 296.13.$

Phân đoạn: $I(\text{phân đoạn}) = \log_2(26167) \approx 14.68.$

Các chuyển vị và đảo ngược từ: $I(\text{chuyển vị}) = \log_2(208) \approx 7.7.$

Vật thay thế: $I(\text{vật thay thế}) = \log_2\left(\binom{340}{25} \cdot 27^{25}\right) \approx 244.12.$

Tổng cộng: I(khóa) ≈ 562.62 bằng cách cộng 4 đóng góp trên.

Theo lý thuyết của Shannon, các ký hiệu bản mã được cho là có phân phối đều và giờ đây giả định mật mã Zodiac-340 cũng vậy. Khi đó nội dung thông tin của một bản mã gồm k ký hiệu là $k \log_2 63 \approx 5{,}98 \cdot k$ bit. Đối với Zodiac-340, sẽ là $340 \cdot \log_2 63 \approx 2032{,}28$ bit, ta có:

$$\log_2(\text{len}) = \log_2(2032{,}28) \approx 10{,}99 \approx 11.$$

Trong công thức ở Mục 2, entropy của ngôn ngữ H(ngôn_ngữ) không đề cập đến bản mã, mà là bản rõ của mật mã, và không liên quan trực tiếp đến công sức giải mã. Đầu tiên phải xác định độ dài của bản rõ. Có thể giả định nó là 340 chữ cái, nhưng điều đó không chính xác.

Bằng các phép thay thế và hoán vị, ta sẽ nhận được một đoạn có 340 chữ cái, nhưng chắc chắn đó không phải là một văn bản tiếng Anh. Nó (gần như) trở thành một văn bản tiếng Anh nếu chúng ta chèn 90 khoảng trống một cách thích hợp, như đã thực hiện ở trên. Do đó, bản rõ bao gồm 430 ký tự trong một bảng chữ cái có 27 ký tự, bao gồm cả khoảng trống. Nói chung, độ dài từ tiếng Anh trung bình được ước tính là 4,5 chữ cái khác với ô trống. Do đó, một văn bản tiếng Anh gồm ký tự có thể giảm xuống còn $k =$ $(1 - 1/4{,}5)$ ký tự khi xóa bỏ các khoảng trống. Nói cách khác, một văn bản rút gọn có k chữ cái tương ứng với một văn bản thông thường có $= 9k/7$ chữ cái. Và thực sự, phân số $9/7 \approx 1{,}286$ khá khớp với giá trị $430/340 \approx 1{,}265$. Do đó, chúng ta sẽ lấy $k \cdot 430/340$ chữ cái làm độ dài của một bản rõ được mã hóa bởi k ký hiệu.

Entropy của ngôn ngữ

Thành phần duy nhất cho (*) vẫn còn thiếu là entropy ngôn ngữ H(ngôn_ngữ). Có thể nói, đối với một không gian xác suất phức tạp, các văn bản bằng ngôn ngữ tự nhiên như tiếng Anh, việc áp dụng công thức $-\sum_{a \in A} p_a \log_2(p_a)$ đã đưa ra ở trên không phải là độ đo thích hợp. Công thức này chỉ tính đến sự phân bố tần số trên các chữ cái riêng lẻ và được gọi là monogram entropy (entropy của một chữ cái). Nó bằng khoảng 4,1 trong một số lĩnh vực văn học thông thường. Nhưng có một số vấn đề khi ước lượng entropy của tiếng Anh như vậy. Chẳng hạn, ký tự thường gặp nhất trong văn bản tiếng Anh bị bỏ qua: khoảng trống ␣.

Kho dữ liệu ngôn ngữ Zodiac có chứa tất cả 14859 chữ cái và [2] đã đưa ra kết luận: Entropy của nó có thể được ước tính là khoảng 1,8. Việc này dẫn đến

$$k \geq I(\text{khóa})/[\log_2 63 - (430/340)H(\text{ngôn\_ngữ})]$$
$$\approx 562{,}62/[5{,}98 - 1.8 \cdot 430/340] \approx 152{,}03.$$

Khoảng xác định duy nhất của mật mã Zodiac-340 nhiều nhất là 152. Chiều dài thực tế là 340 của mật mã lớn hơn nhiều so với độ dài này.

Bản rõ

Bản rõ đã được dịch ra là:

I HOPE YOU ARE HAVING LOTS OF **FAN** IN TRYING TO CATCH ME THAT WASNT ME ON THE TV SHOW WHICH **BRINGO** UP A POINT ABOUT ME I AM NOT AFRAID OF THE GAS CHAMBER **BECAASE** IT WILL SEND ME TO **PARADLCE** ALL THE **SOOHER** BECAUSE **E** NOW HAVE ENOUGH SLAVES TO **WORV** FOR ME WHERE EVERYONE ELSE HAS NOTHING WHEN THEY REACH **PARADICE** SO THEY ARE AFRAID OF DEATH I AM NOT AFRAID BECAUSE I **VNOW** THAT MY NEW **LIFE IS** LIFE WILL BE AN EASY ONE IN **PARADICE** DEATH

Các khoảng trống đã được chèn vào một cách thích hợp. Các lỗi chính tả ở nguyên bản đã không được chỉnh sửa. California đã sử dụng phòng hơi ngạt vào thời điểm đó để thực hiện hình phạt tử hình.

Khi tính đến các thay đổi bất quy tắc, chúng ta có bản rõ là

I HOPE YOU ARE HAVING LOTS OF FUN IN TRYING TO CATCH ME THAT WASNT ME ON THE TV SHOW WHICH BRINGS UP A POINT ABOUT ME I AM NOT AFRAID OF THE GAS CHAMBER BECAUSE IT WILL SEND ME TO PARADLCE ALL THE SOOHER BECAUSE E NOW HAVE ENOUGH SLAVES TO WORK FOR ME WHERE EVERYONE ELSE HAS NOTHING WHEN THEY REACH PARADISE SO THEY ARE AFRAID OF DEATH I AM NOT AFRAID BECAUSE I KNOW THAT MY NEW LIFE WILL BE AN EASY ONE IN PARADISE DEATH

Bản dịch tiếng Việt:

TÔI HY VỌNG BẠN ĐANG CÓ RẤT NHIỀU NIỀM VUI TRONG KHI CỐ GẮNG BẮT TÔI ĐÓ KHÔNG PHẢI LÀ TÔI TRÊN CHƯƠNG TRÌNH TRUYỀN HÌNH ĐIỀU NÀY ĐƯA RA MỘT ĐIỂM VỀ TÔI TÔI KHÔNG SỢ PHÒNG HƠI NGẠT VÌ NÓ SẼ ĐƯA TÔI ĐẾN THIÊN ĐƯỜNG SỚM HƠN VÌ BÂY GIỜ TÔI ĐÃ CÓ ĐỦ NÔ LỆ ĐỂ LÀM VIỆC CHO TÔI NƠI MÀ NHỮNG NGƯỜI KHÁC KHÔNG CÓ GÌ KHI HỌ ĐẠT ĐẾN THIÊN ĐƯỜNG NÊN HỌ SỢ CHẾT TÔI KHÔNG SỢ BỞI VÌ TÔI BIẾT RẰNG CUỘC SỐNG MỚI CỦA TÔI LÀ CUỘC SỐNG SẼ DỄ DÀNG TRONG CÁI CHẾT THIÊN ĐƯỜNG

Tài liệu tham khảo

[1] http://antoanthongtin.vn/mat-ma-dan-su/sau-51-nam-cuoi-cung-mat-ma-zodiac-da-bi-pha-107606

[2] Joachim von zur Gathen, Unicity distance of the Zodiac-340 cipher, https://eprint.iacr.org/2021/1620