

# 黄道十二宫杀手的密码

2020211346

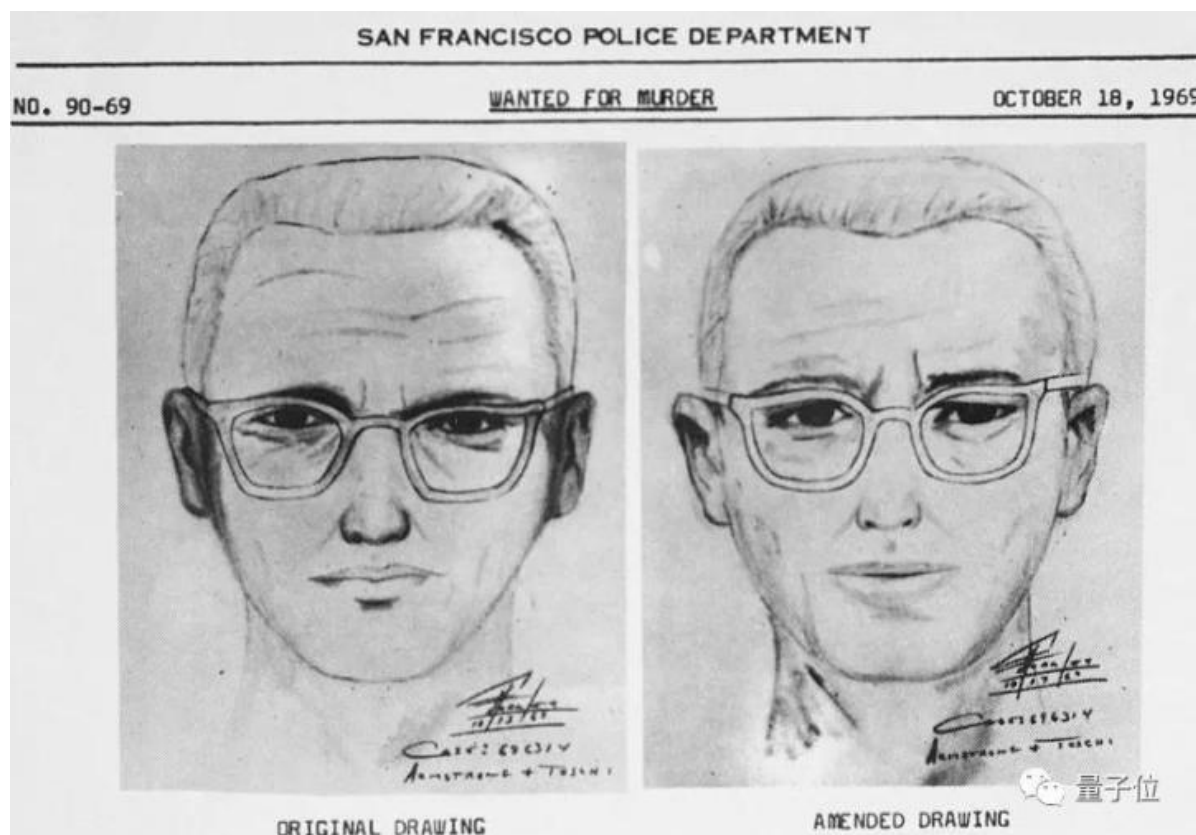
倪玮昊

## 起因

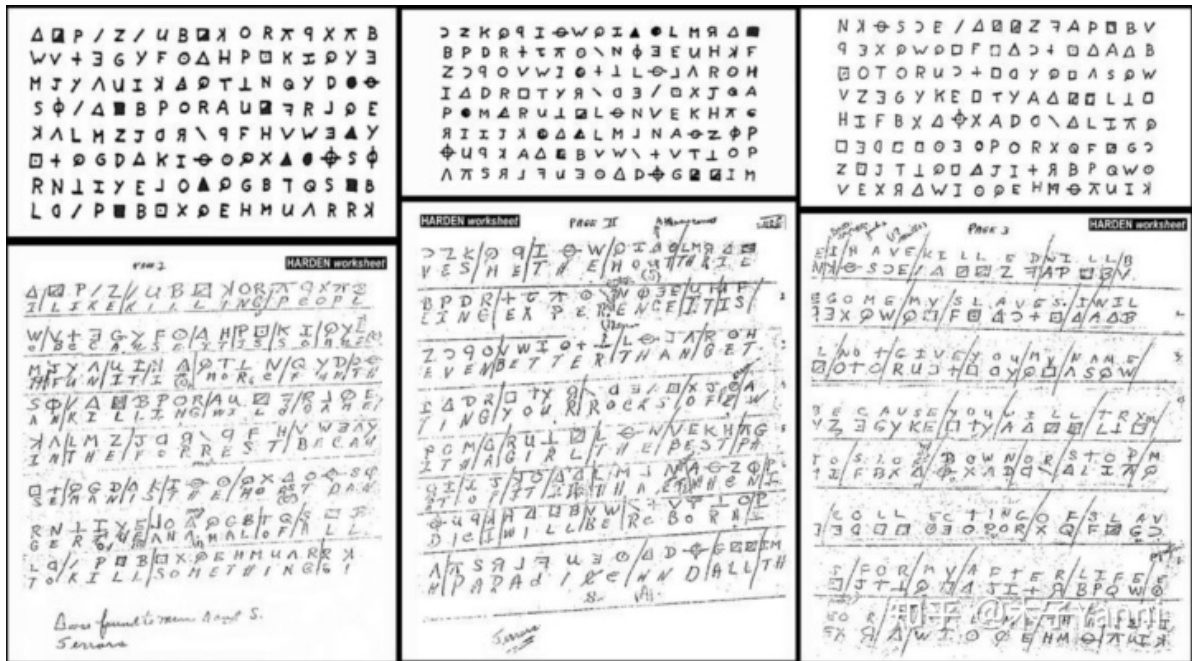
2020年12月，FBI证实了一个令人关注的消息：所谓“黄道12宫杀手”51年前发送给《旧金山纪事报》的一封信件已被破解。这封信中有340个密码符号，被称为“340密码”。破解这封信密码的人包括来自美国弗吉尼亚州的网页设计师David Oranchak，以及澳洲应用数学家Sam Blake和比利时的仓库经理、身兼数码破解工程师的Jarl Van Eycke。近日，破解人之一Sam Blake超详细地公开了密码破解过程，引起了全世界的关注。而之所以能引起如此巨大的轰动，是因为这个杀人案过于有名了，因为其变态的杀人手法和喜欢留下晦涩密码而闻名于世界。

## 案件和两次密码

黄道杀人魔的故事发生在于20世纪60年代末期，在1968年，一个自称“十二宫杀手”的人，使用枪支和刀片，在美国旧金山湾区制造了一系列凶案，凶手还两次打电话给警方，略带嘲讽的报告自己的谋杀罪行。作案期间，这名连续杀人犯先后给媒体寄出了几十封信，内容大多是警方未公开的细节和犯罪证据。其中包含的几封密码信里，引起广泛关注的有Z408和Z340，后者更是挑起了一场长达51年的解密游戏。



Z408密码信出现在1969年8月1日。在此之前，凶手已经制造了两起凶案，分别袭击了一对情侣，导致三人死亡，一人生还。这封密码信混合了字母、符号和数字，全文共408个字符，被拆成等长的三部分，分别寄给了三家不同的报社。发件人在信中威胁说，如果不把密码刊登出来，他就会“整个周末到处杀人，杀完一个再继续，直到杀满十二个为止”。尽管警方根本无法确认这封信就是出自凶手，但再三斟酌后，这封密码信还是如凶手所愿，被刊登在报纸上。8月8日，距离报社收到信仅一周时间，一名名叫哈登教师和他的妻子贝蒂就破解了Z408密码。



破解出的 Z408 内容如下：尽管密码被破解，但其中没有任何有助于破案的线索。

“我喜欢杀人，因为这比在森林里杀野生动物要有趣得多，因为人类是最危险的动物，杀人给了我  
最刺激的经历，这比和一个女孩一起把石头扔下来还要好得多。最棒的是，当我死后，我会在天堂  
里重生，我杀死的人会成为我的奴隶。我不会给你我的名字，因为你会试图下去，或者为了我的永  
生而骑在我的奴隶身上。”

1969 年 11 月 8 日，时隔三个月，十二宫杀手寄出了密码信 Z340，全文共 340 个字符，比上一封略短  
一些。这一封密码信，看似与上一封是同一种密码，但显然，上一封密码信的破解速度激怒了凶手，这  
一次，凶手在其中精心设计了很多花样，在当时很多著名数学家都尝试对密码进行破译，但是没有效果。  
直到 1974 年，关于“黄道十二宫杀手”的信件彻底消失了。后来的十几年，警方一直没有放弃对这封密码信  
的破译，为此专门找来了大学教授，军队的密码专家，以及 FBI 的调查员，可都无工而返。



直到离这封信寄出50年之后的现在,人们才成功破解了这个复杂的密码

## 破解

澳大利亚数学家Sam Blake创建了65万种密码符号的组合,并将所有的组合运行在了由比利时程序员Jarl Van Eycke开发的一款密码破译程序AZdecrypt上面,希望借此找到杀手加密信息的手法。当65万种密码组合被放入密码破译软件后,软件立刻开始尝试破译,很多天过去了,三个人终于在无数个无效解法中,发现了一个似乎含有少量具体单词的解法,包括‘希望你’、‘试着抓住我’、‘或者是毒气室’。但除此之外的其他字符,看上去依然毫无意义。



EHOPE YOU ARE HE SING IST TORRA ENN  
TRYING TO CATCH METH AFTAINT MT ON THE  
 TS SHOT WHICH BRINGS UP ALS IN TABS IT  
 ME NAME OF AR HEED OR THE GAS CHAMBER  
 BECA ATE IT WILD VENT ME ROLER A DICE  
 AI I THE VS SHEN BECAUSE TOO WHA SEEN  
 TIGHT DESERTS WORS ROS ME THERE  
 EVERYONEED HE HAS NOTHING THEN THEY HE  
 ACH PARADICT IS THEY ALREARE AND NORDER  
 THER AMEO EARRE AND BECAUITE IS YOT TV  
 HAT MR NEWE ITLE NEVER IND BAEYN NEIA  
 AT A HOE CDR PET

知乎 @木子Yanni

根据已有出现的少量正确字符，数学家 Sam Blake 对密码进行拆分，前两部分各 9 行，第三部分 2 行。接着，Sam Blake 用对角线的方式，对三部分分别进行了重新排列。

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

153	162	171	180	189	198	207	216	225	234	243	300	301	302	303	304	305
284	292	154	163	172	181	190	199	208	217	226	235	244	252	260	268	276
269	277	285	293	155	164	173	182	191	200	209	218	227	236	245	253	261
254	262	270	278	286	294	156	165	174	183	192	201	210	219	228	237	246
238	247	255	263	271	279	287	295	157	166	175	184	193	202	211	220	229
221	230	239	256	264	272	280	288	296	158	167	176	185	194	203	212	248
204	213	222	231	240	249	257	265	273	281	289	297	159	168	177	186	195
187	196	205	214	223	232	241	250	258	266	274	282	290	298	160	169	178
170	179	188	197	206	215	224	233	242	251	259	267	275	283	291	299	161

309	308	307	306	310	311	312	313	315	314	317	316	318	319	320	321	324
323	322	326	325	334	333	332	331	330	329	328	327	335	336	337	338	339

知乎 @木子Yanni

得到了组合后的密码,并将出现过的单词进行固定,对没有出现过多部分破译,同时根据凶手一些访谈记录和语言习惯对一些词语进行倒拼.

H+M▲I C V □ K E B + ▣ ● X • L  
Q R ϕ U V F F ⊕ Δ < > ■ Z O P > L  
ϕ M 9 O 6 9 + ⊙ I 6 + J ▣ W O P D  
■ ⊙ 8 ∧ D ϕ + ⊙ ϕ ● J + V W ⊕ + X  
9 + 7 Z P Y L R / ▲ K T R X • ■ K  
□ R ⊙ ■ ⊙ I < ⊕ ⊙ Δ ∧ ▣ O F ⊙ ▣ H  
S M F π + B L K J 9 + J ⊙ □ ⊃ T 7  
B 9 ⊕ O U N Y 6 ⊕ Y Δ ⊥ - ⊃ Y A ⊙  
N π ∧ T ▣ X ⊕ ⊙ Q 9 ⊃ J Q Q 6 + ⊙

知乎 @木子Yanni

接下来,他们又用同样的方法,对第二部分进行破译,然而得到的结果中,仅能看出个别单词,比如“奴隶”、“天堂”、“害怕”等。

SOOHENBECAUSEEOOW  
HAVEENSUGHSLAVERT  
OWORVFOVMEWHEREES  
ERYONEELHEHASNOTH  
INGWHENTHEYREACHP  
AYALICESOTREYALRE  
AFAAIDIOFLETTHIFA  
MNOEAFREAI DBNCAUI  
SEIVYOWTSHATMRNEW

知乎 @木子Yanni

按照“倒拼”的思路，他们先对第三部分的词汇进行了拆分。接着，“倒拼”其中不正确的词汇，一个完整的句子出现了：在天堂，生命将会是一个简单的过程。到这一步，几人翻回头去看还未完整破译的前两部分，发现，凶手出现了一些拼写错误，比如把「NOW」写成了「OOW」，「FOR」写成「FOV」，他们对内容进行一些更正后，一篇完整的译文出现了。



I HOPE YOU ARE HAVING LOTS OF FUN IN TRYING TO CATCH ME

我希望你抓我的时候玩得很开心

THAT WASNT ME ON THE TV SHOW 电视上那个人不是我

WHICH BRINGS UP A POINT ABOUT ME 这让我想到了一个问题

I AM NOT AFRAID OF THE GAS CHAMBER 我不怕毒气室

BECAUSE IT WILL SEND ME TO PARADICE ALL THE SOONER 因为它会让我更快进入天堂

BECAUSE I NOW HAVE ENOUGH SLAVES TO WORK FOR ME 因为我现在有足够的奴隶为我工作

WHERE EVERYONE ELSE HAS NOTHING WHEN THEY REACH PARADICE 当其他人到达天堂时，他们一无所有

SO THEY ARE AFRAID OF DEATH 所以他们害怕死亡

I AM NOT AFRAID BECAUSE I KNOW THAT MY NEW LIFE IS 我不害怕，因为我知道我的新生活

LIFE WILL BE AN EASY ONE IN PARADICE DEATH 在 PARADICE，生命将会是一个简单的过程

知乎 @木子Yanni

## 后续

David Oranchak 表示，凶手在对信息加密前，对信息先做了一些处理，比如倒拼等，这也是为什么在长达半个世纪的时间里，密码都没有被破译的一大原因。在破解视频的开头，他们写了这样一段话：“我们所做的这些努力，是为了被杀手杀死的人们及其后代，我们希望正义会取得最终的胜利。”而尽管这封密码信的破解，并没有给案件带来有价值的线索，但能解开长达半个世纪的困惑，价值也不容小觑。同时美国联邦调查局表示，“黄道十二宫杀手”案仍在调查中，他们会努力查明真相，给受害者公道。

这段略显戏剧横跨半个世纪的密码破译故事也给我带来了很大的启发，在这个故事中，密码成为了杀人犯宣泄欲望和优越感的工具，而由于技术的落后，没有人有能力去制裁他，但幸运的是，在现代高算力机器的支持以及密码破译技术的进步下，这些邪恶终于暴露在阳光之下。这也是密码学的伟大之处，在善良的人的手中，可以去用这项技术去拯救更多的人，这也给了我更多的动力去了解和学习密码学。

