Telephone Codes and Safe Combinations: A Deadly Duo

(b)(3)-P.L. 86-36

[redacted]

~~(C)~~ [redacted]

I. PROLOGUE

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted] According to the manufacturer, a U S Government Security Container, Class 6 Cabinet, under the tests defined in Federal Specification, AA-F-358f affords protection for

1 Thirty man-minutes against surreptitious entry

2 Twenty man-hours against manipulation of the lock

3. Twenty man-hours against radiological attack

4 No forced-entry equipment

These standards are actually set by the General Services Administration (GSA) and apply to all federal agencies, including NSA No reference is given to the classification of material that may be stored in these safes [1]

1 ~~(C)~~ [redacted]

(b)(1)
(b)(2)
(b)(3)-P.L. 86-36

Approved for Release by NSA on 04-04-2008, FOIA Case # 51705

(b)(1)
(b)(2)
(b)(3)-P.L. 86-36

(U) As the above list indicates, there are a variety of ways to crack a safe. The oldest and most reliable system is the brute-force method. With proper equipment (crowbars, welding torches, pneumatic drills, sledgehammers, plastic explosives, and dynamite), you can force even the toughest safe open in just a few minutes. The high reliability and low cost of the brute-force method make it a favorite of bank robbers and jewelry thieves. However, because of its high visibility and low aesthetic appeal, the brute-force method is frowned upon in the intelligence community. Forced entry is a sure sign that a safe has been tampered with and is a dead giveaway to the presence of a hostile agent working in our midst.

(U) Most spies and sophisticated criminals will opt for one of the more low profile approaches that fall under the category of surreptitious entry. As the name implies, "surreptitious entry" means any method of penetration that leaves no trace of the compromise. This could involve using various probes and meters to correctly ascertain the combinations, or perhaps jimmying the lock without dialing any combination at all. As long as the penetrator does not leave any noticeable trace of his activity, he has effected a surreptitious entry.

~~(C)~~ [redacted]

~~(FOUO)~~ [redacted]

II. THE EXPOSÉ

A. *Following the Letter of the Law*

~~(FOUO)~~ [redacted]

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

~~(C)~~ [redacted]

Fig. 1. ~~(C)~~

~~(C)~~ [redacted]

2 (U) This figure presupposes 'Wide' to mean $|x_i - x_j| \geq 10$, and 'Not near zero' to mean $10 < x_i < 90$

(b)(1)
(b)(2)
(b)(3)-P.L. 86-36

B Casual Code Combos

(U) Given the official rules as a baseline, the astute safe owner must develop some system for choosing a particular combination from amongst the 38,720 possibilities There are many systems for choosing combinations For example, one could choose all primes (e g , 31-87-53) or numbers with the same "ones" digit (e g , 32-82-52) A good decision for the indecisive person is to use a random number generator At any rate, most users employ some mnemonic in order to make the numbers easier to remember Indeed, forgetting your combination reduces your safe to a useless piece of furniture, rather than a depository for information

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

C Breeding the Master List

~~(FOUO)~~ In order to create this list, we initially tried to consult an on-line dictionary Unfortunately, our network didn't have a good system dictionary – at least no adequate one This hurdle was easily surmounted Using various sort commands and a hack developed by [redacted] we were able to combine four system dictionaries, thus obtaining a putative list of 30,194 six-letter "words" This list had to be pruned by removing words that resulted in illegal combinations This reduced our putative dictionary to 2,113 words, the only specifications being those found in *NSA/PMM* 30-2 together with the mildly restrictive Lo-Hi-Lo rule

~~(C)~~ [redacted]

(b)(1)
(b)(2)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

course, we must assume that the person knows how to spell[3]

(U) We first assumed that the typical user's vocabulary, though it might be relatively large, is significantly smaller than the unabridged *Oxford Dictionary*. Therefore, we threw away a few actual words that are very uncommon these included place-names such as Iturea and Inchon, scientific names such as biotin and octoid, and abstruse theological terms such as anomia We also threw out most two- or three-word combinations such as "all the," "on file," and "so be it," although we kept "nofair" and most hyphenated words such as "cave-in," "move-in" and "head-on"

(U) On the other hand, we kept many possible words that perhaps would not be frequently used These included most personal pronouns (Harlan, Indira, Tybalt), compound words (mugful, outhit, unbait), and certain abbreviations (sgtmaj, theyre)

~~(FOUO)~~ [redacted]

(U) We next divided the Master List into three sublists, depending upon how common the words were The least common and most difficult words were grouped into a scholarly section called the *Savant* list The next most common words, for people with more limited vocabularies, we grouped into a section appropriately dubbed the *Dimwit* list The most common words of all, ones that any first grader would know, were put into a section called the *Stooge* list

(U) Let's take a look at what sort of words don't make the *Dimwit* or *Stooge* list The *Dimwit* and *Stooge* lists consist of those combinations normally used by a person with limited knowledge and intelligence Such a person would probably be unfamiliar with the Bible, thus ruling out such words as Hebron and Gibeon He probably wouldn't have any interest in science either, thus eliminating such words as bromic and dipole Nor would he likely be versed in medicine (ampule, aortic), literature (Aeneid, Hecate), geography (Canoga, Nassau), chemistry (butane, picric), biochemistry (casein, lipids), coding theory (baudot), carpentry (bevels, coving), law (lessee, hereat), biology (oocyte, larvae), zoology (conchs, botfly), agronomy (borage), philosophy (Anselm), social science (Aussie, Ubangi, Kenyan), religion (cupula, Fatima), grammar (gerund), aesthetics (Ionian), horses (dapply), ships (dinghy), mountaineering (escarp), carpentry (lathed), American Indians (Kiowas), fine confection (nougat), or medieval armor (greave)

3 (U) Ironically, if the person is so illiterate as to not even know how to spell, our plan of attack becomes much more difficult, since we must expand our dictionary to accommodate all the misspellings

(b)(3)-P.L. 86-36

D. The Attack

~~(FOUO)~~ [redacted]

~~(FOUO)~~ For years, top-class criminals and spies have successfully employed automatic dialers to break into safes. They are also used by legitimate locksmiths to open safes without ruining them. Autodialers work quite well, so well in fact that having one without a license is considered possession of burglary equipment and is a felony offense. These high-speed machines can zip through an amazing ten combinations per second. The ITL-1000 is a commercial brand that has been verified against the MOSLER 300 series in 30 hours. Commercial machines have not been verified against the Sargent & Greenleaf 8400 and 8500 series.

~~(C)~~ [redacted]

~~(FOUO)~~ At any rate, we have assumed that an autodialer can try about four combinations per second, about sixty times as fast as a dexterous human. The expected crank time (i.e., the average time needed to open a safe) for both the manual and autodialer methods is summarized in figure 2.

(b)(1)
(b)(2)
(b)(3)-P.L. 86-36

List	Number of		Expected Cranking Time	
	Words	Combinations	Manual	Autodialer
Savant	244	224	28 minutes	28 seconds
Dimwit	166	122	15 minutes	15 seconds
Stooge	176	130	16 minutes	16 seconds
Total	586	476	59 minutes	59 seconds

Fig. 2. (C) Expected crank times

III. GALERIA

(U//FOUO) ~~(U)~~ Here we present the 476 most probable safe combinations and their associated six-letter words This "Master List" is broken up into three subsections least likely used, more likely used, and most likely used The first part of each section lists the actual combinations (in order down the columns), the second part records the associated six-letter words A particular combination may refer to more than one word For instance, in the most likely section [redacted] See if a past or present combination of yours makes our list[4]

(b)(3)-P.L. 86-36

4. (U) If you happen to notice a rather difficult word in the *Dimwit* or *Stooge* list, remember that it probably corresponds to a simple word that mapped to the same combination

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

IV EPILOGUE

~~(C)~~ [redacted]

~~(C)~~ [redacted]

~~(FOUO)~~ Fortunately for security, a new generation of locks is now on the horizon electronic locks These locks may be immune to exhaustive attacks For example, the Moss-Hamilton electronic lock shuts down for forty seconds after five failed attempts [5] However, it is clear that weaknesses of the current combination locks will provide thieves and spies fruitful safecracking possibilities for many years to come

(b)(1)
(b)(2)
(b)(3)-P.L. 86-36

5 (U) There are also certain mechanical locks that can be set to seize up under an exhaustive attack

(b)(3)-P.L. 86-36

Appendix A

Combinations in the Fast Lane

(U) A time-conscious safe user should also address the question of which combinations are easiest to dial. For the purpose of speed, the best combinations are the ones that use just 0s and 5s, and that minimize the radial distance traveled by the dial in order to open the lock. By this standard, the all-around best combination is 15-5-10 which has a total radial distance of 325 digits. However, the use of this combination is not recommended, if only for the simple reason that the numbers are not widely enough spaced to guarantee against failure of the lock.

(U) Let us then assume that a certain combination follows the formal set of rules given by NSA in figure 1. Based upon these rules, it is possible, given three numbers x_1, x_2, x_3, to calculate the maximum, minimum and average dialing distances. This distance is given by $d = x_1 + 2(x_3 - x_2) + 100n$. In figure 3 these values are tabulated for the various order relationships among the numbers.

	Rule			
	$x_1 < x_2 < x_3$ $n=4$	$x_1 < x_2, x_3 < x_2$ $n=5$	$x_1 > x_2 > x_3$ $n=4$	$x_1 > x_2, x_3 > x_2$ $n=3$
Max	522 (16-31-84)	524 (54-84-69)	454 (84-31-16)	505 (69-16-84)
Min	446 (16-31-46)	395 (31-84-16)	378 (84-69-16)	376 (46-16-31)
Avg	474.6	463.9	425.4	436.1

Fig. 3. (U) Radial dialing distances

(U) There is a popular misconception that the Lo-Hi-Lo rule reduces the radial distance that the user must spin the dial in order to open the lock. Although the absolute fastest combination that follows all the rules (46-16-31) does indeed follow the Lo-Hi-Lo rule, on the *average*, the "$x_1 > x_2 > x_3$" rule will result in a faster combination. In fact, the adoption of this rule as the official NSA standard could save the government thousands of dollars over the next few decades.

(U) Let us compare the average time saved over an agency-long career for the conscientious employee who uses the efficient $x_1 > x_2 > x_3$ rule as opposed to the unenlightened employee who unwittingly uses the slower $x_1 < x_2 < x_3$. Let us assume that it takes about one second per revolution of the dial. Assuming that an employee opens his safe about once a day ~~during each~~ workday, the faster combinations lead to a savings of about one-half second per day. Now there are about 220 work days per year, once you take into account fifty-two weekends, twenty days of vacation, ten paid holidays, and ten days of sick leave. Assuming the average career is about twenty years, the grand total of time saved is

$$\left(\frac{220\ days}{year}\right)\left(\frac{\frac{1}{2}\ second}{day}\right)\left(\frac{20\ years}{career}\right)\frac{(1\ hour)}{(60\ minutes)}\left(\frac{1\ minute}{60\ seconds}\right) = 0.6\ hours$$

(U) In terms of dollars, this is quite significant. Let us assume that the average Agency employee earns $25 per hour. Then for for every 1,000 employees, the savings from using the fastest combination choice is an amazing

$$\left(\frac{0.6\ hours}{employee}\right)\left(\frac{\$25}{hour}\right)(1{,}000\ employees) = \$15{,}000.00\,!$$ [6]

(U) As a final note, one could also survey all possible [redacted] to see which of those is fastest. Assuming, as we have, that the safe user employs the Lo-Hi-Lo rule, the fastest combination is 52-22-37, which corresponds to [redacted] with a rotational distance of just 382 units. We recommend that this word be adopted as *the* quick-and-dirty [redacted] safe combination for safe users worldwide.

(b)(3)-P.L. 86-36

6. The authors hope [perhaps somewhat naively – Ed.] to split a $15,000 cash award for pointing out this little-known fact.

Appendix B

Distribution of Words According to Length

(U) It is interesting to note that the English language is replete with six-letter words. Only seven-letter words are more common. There are actually about 300,000 words in the English language (when even the most erudite gems have been accounted for), of which an estimated 45,000 have six letters. Figure 4 depicts the *approximate* distribution of words with various numbers of letters. Although this bar-graph is based on a rather limited system dictionary of only 25,134 words, it indicates that about 15 percent of all words in common usage have six letters.

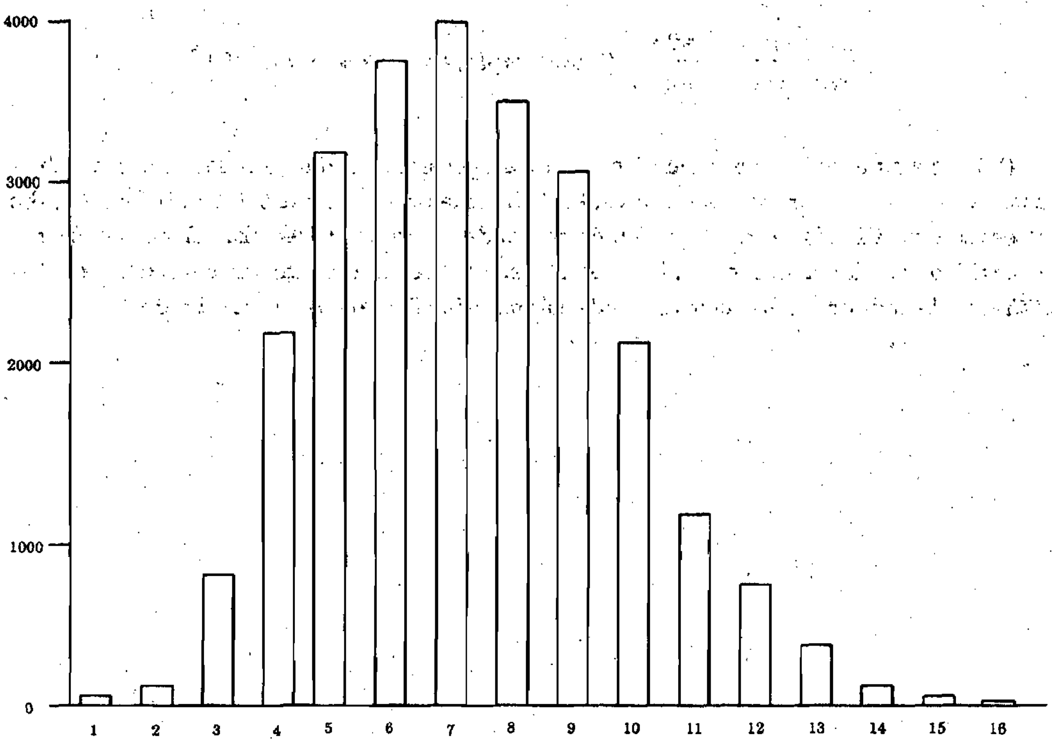

Fig. 4. (U) Number of words for each word length

~~(FOUO)~~ Four- and ten-letter words are about half as common as the ubiquitous six- and seven-letter words. Words with fewer than four or greater than ten letters are dramatically more scarce. In fact, the number of words decreases by roughly a factor of two for each letter in excess of ten or fewer than four. This indicates that mnemonic systems using four- to ten-letter words are roughly comparable to a six-letter system. Obviously, good mnemonic systems should have a large sample space of words to draw from. Therefore, systems that use fewer than four letters or more than ten letters are less than optimal.