A 256-part list for memorising 128-bit keys by constrained choice

Stephen Hewitt

August 2018
Version 1

Copyright (c) 2018 Stephen Hewitt

This document is provided in the hope that it will be useful but it is provided “as is” with NO WARRANTY, not even of merchantability or fitness for any particular purpose.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3, which terms include under Section (1) acceptance and incorporation of the above warranty disclaimer. A copy of the licence is at http://www.cambridgeclarion.org/gfdl-1.3.html. If you received this document from somewhere other than cambridgeclarion.org then you should have received a copy of the licence with it. (Including a copy of the licence itself in further distribution is a licence condition). This document has no Invariant Sections, no Front-Cover Texts and no Back-Cover Texts within the meanings defined in the licence.

Introduction

This document is intended to help memorise cryptographic keys and other strong secrets using the method introduced in the following article.

“How to remember a 128-bit key using constrained choice”, Stephen Hewitt, August 2018
http://www.cambridgeclarion.org/pw2.html

For information on how to use this document see the article.

This version of this list uses the system of abbreviation of taking the first three letters of each word. If the word contains less than three letters it is padded with “x”

Note that Appendix 1 (Inverse Lookup) allows you to look up an abbreviation and recover the value of the byte of the key.

Key to the partition headings

For example in the heading “0x0e = 11/66;46 = A;O = 14”

0x0e Value of this byte of the key in hex, written in C/C++ style with leading 0x
11/66;46 The dice outcome for those that wish to use dice to generate the key
A;O The equivalent letter bead outcome
14 Value of this byte of the key in decimal

The {} brackets that follow contain the allowed abbreviations.

Words and their abbreviations, a list in 256 parts

0x00 = 11/66;11/66 = A;A = 0 { con } con conceit conceive concept concern concert concession concierge concrete concubine condemn conditions condo condom conduct cone conference confetti configure confirm conflict congress conifer conjure conker connect conquer consent consider console conspiracy construct consumer contact contain contest context continue contraception contract control convention convey convince convoy

0x01 = 11/66;12 = A;B = 1 { com } coma comb combat combine come comedy comet comfort comic comma command comment commerce commission committee commode commodity common communist community commuter compact companion company compare compass compassionate compel compensate compete complain
0x7f = 24;56 = H;P = 127 \{ adh amb gry gyr hig jui mix ori tor \} adhesive ambassador amber ambiguity ambition ambulance ambush gryphon gyre gyro high highland highlight highway juice mix morphology orientation original orion tor orah torch torpedo torque torrent torso tortellini tortoise tortoiseshell torture torture

0x80 = 25;11/66 = I;A = 128 \{ ada fac gog goy hap hav moa osc sum \} adaptor facade face faceplate facial facility facsimile fact faction factotum faculty goggles goy happen happy havana haven haversack havoc hoon moat oscar oscillator oscilloscope sum summary summer summit summons sump

0x81 = 25;12 = I;B = 129 \{ gan gnu hau inc iri lac nai put wus \} gander gandhi gang gangster gnome gua haul haunt inc incarcerate incense incessant incite include income increase increment incur iridescence iris irish lace lack lacquer lactase lactose nail naivety putty wuss

0x82 = 25;13 = I;C = 130 \{ fis gno haw hyd isl mal mob puw wyw \} fish fishnet fission fist gnome hawk hawser hydra hydrate hydrdraulics hydrocarbon hydrochloric hydrogen islam island isle mal- malaria malawi malaysia maldive male mal mali mallard mallet malt malta mob mobile puzzle wyvern

0x83 = 25;14 = I;D = 131 \{ acu gue hec iro lam ner pyg rom win \} acute guernsey guerrilla guess guest heckler hectare iron ironmonger irony name namibia nerve pygmy roma roman romance romania rome romp win winch wind windmill window windscreen wine wing wink winkle winter

0x84 = 25;15 = I;E = 132 \{ emb geo hed hes luc mak mea ova rex \} embargo embark embarrass embassy embed ember emblem embody embrace embroider embroidery embryo geography geology geometry geophysics hedge hedgehog hesitate luck make makeup meadow meal means measure meat oval ovary ovation rex

0x85 = 25;16 = I;F = 133 \{ cow git hee hir his muc pas pav xia \} cow coward cowboy cower cowl cowpox git heed heel hire hispanic hiss histogram history muck mucus pass passage passenger passion passive passport password past pasta pastor pasture pave pavement pavilion xian

0x86 = 25;23 = I;G = 134 \{ cov gig hen nan noa pec raj sur xma \} covariance cove covenant cover covert covet gig gigabit giggle gigo hen henna nanny nano- noah pecan peck pecs raj surf surface surge surgery surname surplus surprise surrogate surround survey survivor xmas

0x87 = 25;24 = I;H = 135 \{ cos eav kar mud pea piv rak rap xyl \} cosh cosmetic cosmos cost costume cosy eaves eavesdrop karaoke karate karma mud muddle pea peabody peace peach peak peal peanut pearl peasant peat pivot rake rapid rapid rap rapper xyllophone

0x88 = 25;25 = I;I = 136 \{ act dro fig hib hik jes mug rai ral \} act dromedary drone droop drop dropout drosophila dross drought drove drown drowsy fig fight figurefigurehead hibernate hibiscus hike jest jesus mug mugger raid rail droop drop wind windmill windscreen wine wing wink winkle winter

0x89 = 25;26 = I;J = 137 \{ gin gis hic ide jog lye map swi \} gin ginger gingivitis ginkgo gist hiccup hickey idea idealist identify jog lye map maple pet petal petition petry peti petrol petticoat swift swing swim swindler swimmer swing swivel

0x8a = 25;34 = I;K = 138 \{ deb gim hie hij idi ram typ unw yak \} deb debate debauchery debilitate debit debrief debris debt debug debunk debut gimmick hierarchy hijab hijack idiom idiomsycrasy idiot idiom rama ramp rampart type typhoid typhus typist typo unwind unwrapp yap

0x8b = 25;35 = I;L = 139 \{ bur hid hil juj kaa paw ran too yal \} burden bureau burger burgundy burial burka burn burp burr burrow burst burundi hide hide hilt jujutsu knock knapsack knapweed knit paw pawpaw ranch randy range ransom rant root tooth yale

0x8c = 25;36 = I;M = 140 \{ att beg hoa ign nir rab rar tos yam \} attach attack attain attempt attend attention attach attire attitude attorney attract attribute beg beget beginning begonia begrudge beguile hoard hoax ignite ignominy ignore nirvana rabbit rabbit rabble rabies rare tosh toss yam

0x8d = 25;45 = I;N = 141 \{ aff gif gor hop jok nig pis toy yap \} affairs affect affidavit affiliate affiliation affirmative affix affiliation afford affray against gift gore goggle gorilla gorse gorse hope joke nigeria niggie night nightcap nightie nightjar nightmare pistachio pistol pistol toy toyota yap

0x8e = 25;46 = I;O = 142 \{ acn ele gia hei hew hov mor nar tuf \} acute elect electric elegant elements elephant elevate eleven giant heifer height heir heist hey hovel hover moral morn morrow morning morocco moron morphine morose morsel mortgage mortuary narcotic narrative narrow tumult tumultuous tuf tuft

0x8f = 25;56 = I;P = 143 \{ ack fid gho het how nut reg rut wri \} acknowledge fiddle fidelity fidget fiduciary ghost heterosexual howl howl nut nutmeg nutrient regard regenerate reggae regime regime regina region regist regreg regret regular tut tutor twister wing wrinkle wrist writ write writhe

0x90 = 26;11/66 = J;A = 144 \{ hul ill ink loz pau pus roz sti twa \} hulk hull ill illegality illegitimate illiterate illuminate illusion illustrate ink lozenge paunch pauper pause push puss pussy pussyfoot rozzle stick stuff stigma stile stilt stilton sting stingray stink stir stitch twang twat
0xb5 = 35:16 = L;F = 181  \{ alc ded fom mis nuz pac reb yah zio \}  alcohol alcove dedicate deduce deduct foment miser mishap mislead miss missile mission mist mistake misterletoe mistress nuzzle pace pacific pack package pact rebate rebel rebirth reboot rebuid rebuke yahoo yahuweh zion

0xb6 = 35:23 = L;G = 182  \{ alm bot dau kaf nyl sle sui wif zip \}  almond alms botany botch bother botox botswana bottle bottom daub daughter daunt kaftan nylon sleeze sled sledge sleek sleep sleet sleeve sleigh sleuth slew suicide suitable suitcase suite suitor wife wifi zip

0xbb7 = 35:24 = L;H = 183  \{ alp ber det kai lev nep nym yaw zir \}  alphabet alps berber bermuda berry detach details detain detect deter detrimental determine determinate detest detliner kaiser levant levee level lever levianith levity levi nepal nephew nephron nepotism neptune nympho yaw yawn zircon

0xb8 = 35:25 = L;I = 184  \{ amm doc fil foc oaf pos syr yes zit \}  ammno ammonia doc dock doctor doctrine document filch file fill filly film filter filter posse possesse possible post postdoc poster postscript posy syria syringe syrup yes yesterday zit

0xbb9 = 35:26 = L;J = 185  \{ ann bud dod fob lef oaf wal yog zod \}  amnesia amnesty buddha buddeliea buddy budge budget budgie dodder Doddle dodge dodgern dodo fob left leftism leftover oak wales walk walkman wall wallet wallpaper wally walnut walrus waltz yoga yoghurt zodiac

0xbaa = 35:34 = L;K = 186  \{ amo aut kak neo oar pee tas yok zom \}  amoeba aminate authenticate author autism auto autobiography autograph automatic autonomy autopsy autumn laki neoconservative neolithic neon neophyte neoprene oar pee peck peckaboo peel peep peer peeee task tasmania taste yoke yokel zombie

0xbbb = 35:35 = L;L = 187  \{ dog fjo lem oas pit tin vis you zon \}  dog dogma fjord lemma lemon lemonade oasis pit pitch pitcher pith pity tin tinder tinker tinkle tinnitus tinsel tint visa visage viscosity viscount vizimu visible vision visit visitor young youth zone

0xbc = 36:12 = M;M = 188  \{ cun cys dol fix nur pho ret zil zor \}  cuneiform cunnulingus cunning cyst cysteine doeck doll dolly dolphin fix nursery phobia phoenix phone phony photospherecence photo photon retail retain retch retina retire retreat retrieve retrotro retrovirus return zilch zillion zoroaster

0xbd = 36:15 = M;N = 189  \{ cul cyt fiv hin jed sal shu zin zuc \}  cull culture cytokine cytology fiver find hinder hindu hinge hint jiddah salad salary sale salmon salon salsa salt salute salvo shudder shuffle shun shunt shut shutter shuttle zinc zucchini

0xbe = 36:16 = M;O = 190  \{ cud dad div dou nec obi roe voy zul \}  cud cuddle cudgel dad dado diva divan diver diverse divert divide dividend divorce divulge double doublet doubleon dougb draft dougbness neck necklace necrophilia nectar obit roe voyage voyeur zulu

0xbf = 36:17 = M;P = 191  \{ bul cuc dag dru obj pal vau zyg \}  bulb bulgaria bulge bulk bull bulletin cuckold cuckoo cucumber dag dagger drudge drug druid drum drunk object pal palace pale palestine palette pall pallet pallor palm palsy vaudeville vault yagote

0xc0 = 36:11/66 = M;A = 192  \{ cry dal neg ont red veg whe yod \}  cry crypt crystal dal dale negative neglect negligence negotiate negro ontology red redeem redevelop redheat redrect redistribute reduce vegan vegetable wheat wheedle wheel wheelbarrow wheelchair wheeze whelk wherry whet whey yodel

0xc1 = 36:12 = M;B = 193  \{ bus dow lay luf obo tex vei wor \}  bus bush bushel business busker bust bustle dawdle dawn lay layer layman layoff layout luftwaffe oboe text textile texture veil vein worcester work workout workshop world warn worry worship worth

0xc2 = 36:13 = M;C = 194  \{ daz dri eli jaz low nat vie yem \}  daze dazzle dribble drier drift driftwood drill drink drip drive drivel drizzle elicit elide eligible elijah eliminate elite elixir jazz low lower lowercase natal national native nature naturist vietnam view yemen

0xc3 = 36:14 = M;D = 195  \{ ama dei nun rej slo und vig yen \}  amateur amaze amazon deism deity nun reject rejoice rejoin rejoinder rejuvenate slob slog slop slope slot sloth slow under undergrad underground underline undermine understand undertake underwear underwater undress vip viper yen

0xc4 = 36:15 = M;E = 196  \{ alt beh dex jaw mat ple voi yeo \}  altar alternative altitude behaviour behed behemoth behest behind behold behoove dexterity dextrorse jaw mat mate material maternity maths matrix matter matress mature plea please pleat pledge plenty voice void yeoman

0xc5 = 36:16 = M;F = 197  \{ ace did gat met oce ten vot wed \}  acetone didactics diddle gate gateau gatecrasher gathering gator metabolism metal meteor meter method methodist metro ocean ten tenant tend tennis tenor tense tension tent tenure totary vote wed wedge wednesday

0xc6 = 36:23 = M;G = 198  \{ cau cod cyp och pin vow wei yet \}  caucasus caucas cauliflower cause caution cod code codeine codex codger codicil codpiece cypress cyprus ochre pin pincer pinch pine pineapple ping pink pinacle pinole pint vow vewl weigh weir weird yet
Appendix 1: Inverse Lookup - abbreviation to partition value in hex

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td>0x00</td>
<td>aabbcc</td>
</tr>
<tr>
<td>abd</td>
<td>0x01</td>
<td>aabbdc</td>
</tr>
<tr>
<td>abe</td>
<td>0x02</td>
<td>aabbeb</td>
</tr>
<tr>
<td>abc</td>
<td>0x03</td>
<td>aabbcc</td>
</tr>
<tr>
<td>ade</td>
<td>0x04</td>
<td>abcdab</td>
</tr>
<tr>
<td>bcd</td>
<td>0x05</td>
<td>bcdbac</td>
</tr>
<tr>
<td>cde</td>
<td>0x06</td>
<td>cdbeab</td>
</tr>
<tr>
<td>def</td>
<td>0x07</td>
<td>cdefbc</td>
</tr>
<tr>
<td>fde</td>
<td>0x08</td>
<td>fdecbd</td>
</tr>
<tr>
<td>edf</td>
<td>0x09</td>
<td>defedc</td>
</tr>
</tbody>
</table>

Note: The inverse lookup table maps abbreviations to partition values in hexadecimal format.