ACE Working Group
Internet-Draft
Updates: 2289 (if approved)
Independent submission
Category: Informational
Expires: 26 August 2025

R. Corbel
Orange Group

22 February 2025

Improvements to the One-Time Password System defined by RFC2289
draft-corbel-ietf-ace-one-time-passwords-00

Abstract

This document aims to submit a few improvements to the RFC2289, which describes a One-Time Password System : interfaces to Secure Hash Algorithms, folding hashes to 64 bits, alternate dictionaries and automatic renewal of authentication parameters will be studied in detail.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 26 August 2025.

Copyright Notice

Table of Contents

1. Introduction

When RFC2289 [0] was published in 1998, and became a Standards Track specification in 2000, it described a powerful One-Time Password system. Many things have changed since that time, notably the way hashes are computed : one distinct interface for each hash algorithm yesterday, only one today. We describe here that unique interface. As a consequence, folding hashes to 64 bits (the length of an One-Time Password or OTP) requires a different technique, which is also described. Finally, we propose a technique for automatically renewing authentication parameters between a user and an OTP authentication server.

Understanding RFC2289 is a requirement.

2. Interfaces to Secure Hash Algorithms

In 1998, only three secure hash algorithms were commonly used : MD4 [1], MD5 [2] and SHA1 [3]. As the security of those algorithms became insufficient, three new secure hash algorithms appeared : SHA256, SHA384 and SHA512 [4]. MD4 is not used anymore. A common interface has been defined by OpenSSL for those five hash algorithms :


```
EVP_MD_CTX * mdctx;
unsigned int dlen;
const EVP_MD * md;
unsigned char digest[EVP_MAX_MD_SIZE+1];
/* algo is a string naming the desired hash. Case insensitive.
   Name is one of "md5", "sha1", "sha256", "sha384" and
   "sha512".*/
md = EVP_get_digestbyname(algo);
mdctx = EVP_MD_CTX_new();

/*Compute the hash. */
memset(digest, 0, sizeof digest);
EVP_DigestInit_ex(mdctx, md, NULL);
EVP_DigestUpdate(mdctx, data, sizeof(data));
EVP_DigestFinal_ex(mdctx, digest, &dlen);
```

```
  /* Free the memory used by the context */
  EVP_MD_CTX_free(mdctx);
```

3. Folding hashes to 64 bits

The lengths of the hashes produced by MD5, SHA1, SHA256, SHA384 and SHA512 are, respectively, 128, 160, 256, 384 and 512 bits. Since the length of an OTP is 64 bits, it is necessary to fold the hashes.

The technique for folding MD5 hashes to 64 bits is taken as is from RFC2289 (Appendix A, pp.12-13) :

```
  /* The MD5 hash */
  unsigned char result[16];
  /* Fold the 128 bit result to 64 bits */
  for (i = 0; i < 8; i++)
    result[i] ^= result[i+8];
```

The technique for folding SHA hashes to 64 bits is a generalization of the one presented in RFC2289 for SHA1. It is designed to be compiled and to run on a 64-bit, Little Endian platform :

```
  /* dlen is the number of BYTES contained in the array pointed
     to by d1. d2 is the array that receives the result of the
     folding. */
  void foldShaTo64(unsigned int dlen, unsigned char * d1,
    unsigned char d2[8]) {
    /* Size of the array pointed to by d1 in number of 32-bit
       words*/
    unsigned int dlen32 = dlen / 4;
```



```
    /* Typecast digest d1 to an array of 32-bit words. */
    unsigned int ld[dlen32];
    unsigned int * pl = (unsigned int *)d1;
    for (unsigned int i = 0; i < dlen32; i++) {
      ld[i] = *(pl + i);
    }
    /* Actual folding to 64 bits. */
    for (unsigned int i = 2; i < dlen32; i++) {
      ld[i % 2] ^= ld[i];
    }
    /* Store the result as a Big Endian value in the output
       array.*/
    int i, j;
    for (i = 0, j = 0; j < 8; i++, j += 4) {
      d2[j+0] = (unsigned char)((ld[i] >> 24) & 0xFF);
      d2[j+1] = (unsigned char)((ld[i] >> 16) & 0xFF);
      d2[j+2] = (unsigned char)((ld[i] >>  8) & 0xFF);
      d2[j+3] = (unsigned char)((ld[i]      ) & 0xFF);
    }
  }
```

We now have the tools for producing 64-bits OTP from hashes computed by any of the five algorithms. Appendix A gives a series of inputs and correct outputs to check the behavior of an implementation of an OTP generator (RFC2289 gives such information for MD5 and SHA1, while Appendix A here gives the information for the same inputs

hashed by SHA256, SHA384 and SHA512 hash algorithms).

The conversion of a 64-bit OTP to a set of six words taken from the RFC2289 Standard Dictionary is based upon the same process (compute a 2-bit checksum from the 64-bit OTP, stick those two bits at the end of the OTP thus producing a 66-bit value; this value is then divided into six slices of 11 bits that allow to address six different words in a 2048-word dictionary).

4. Holes in Alternate Dictionaries

RFC2289 specifies a 2048 English word dictionary (Appendix D p. 19) that can be used by OTP generators for converting a raw OTP expressed in hexadecimal into a set of six different words taken from that dictionary. This feature is designed to ease the authentication by human users.

RFC2289 also specifies a way to use Alternate Dictionaries, that is dictionaries made of 2048 words taken from a language different than English, no word appearing in more than one dictionary. As stated in

RFC2289 Appendix B p.14 :

> "An alternative dictionary of 2048 words may be created such that each word W and position of the word in the dictionary N obey the relationship:
>
> alg(W) % 2048 == N
>
> where
>
> alg is the hash algorithm used (e.g. MD4, MD5, SHA1).
>
> In addition, no words in the standard dictionary may be chosen."

Let’s consider the RFC2289 Standard Dictionary and the Alternate Dictionary defined in this document (Appendix B), made of 2048 French words, and let’s apply the above algorithm to both lists of words, using the five hash algorithms. The results can be found in this document (Appendix C).

For both lists, the collision rate varies from 35% to 37%. This means that on 10 words taken from one of the lists, almost 4 of them share at least two equal (alg(W) % 2048) values. Concretely, every word W of a n-uplet that share the same (alg(W) % 2048) value will be written in the same slot of the 2048-word alternate dictionary, the last word of the n-uplet taking over the first ones. Finally, this techniques leaves (n-1) empty slots or "holes" in the final alternate dictionary.

This MAY lead to a security weakness if an attacker gets to know the alternate dictionary computed, as shown above, from an initial list of 2048 words (every one being different from words in the Standard Dictionary). The alternate dictionary is reduced by 35%, eventually easing the task of guessing one or more words that will appear in the next OTP.

5. Automatic renewal of authentication parameters

By design, OTP’s cannot be used forever by the same user : when the sequence number, decreased at each successful authentication, reaches zero, the user can’t authenticate anymore.

A reset of user’s parameters must be done by providing the server with, at least, a new sequence number and the matching OTP but this is dangerous because this can lead to the generation of the same sequence of OTP’s. This would expose the user to race attacks.

It is then highly recommended that the user provides the server with:
- a different hash algorithm name (at most 10 characters plus the ending zero);
- a new seed (at most 16 characters plus the ending zero);
- a new sequence number (a 4-byte Little Endian unsigned integer);
- and the (first) matching OTP (64 bits i.e. 8 bytes).

1. So, when the user, just authenticated, sees that his sequence number has reached zero, he can simply generate the above values (with the help of a good random number generator when it comes to the new seed and the new sequence number), store them in a 1+40 bytes block, where the first byte codes for the request to renew the authentication parameters, and send the block to the server. The block MAY be encoded in Base 64.

2. Upon receiving the renewal request, the server reads the new values (possibly encoded in Base 64) stored in the block and sends the block back to the user with its first byte indicating the renewal request has been received.

3. Upon receiving the acknowledge block from the server, the user checks that it contains the same values as those stored in the original block. If they are different, the user tries again to send the original block, until three failures occur, or the transmission has succeeded. If the values are the same, the user finally sends the server the original block with its first byte indicating the transaction is ok.

4. The server finally updates the user’s authentication parameters. The user can authenticate again.

This three-way handshake ensures that the server has updated the user’s record with correct data, and that no field receives impossible values (like a corrupted hash algorith name). This algorithm above does not describe the first time initialization of a new user.

6. Security Considerations

Note that the technique described in 5. above allows the user to update his authent parameters anytime, whatever the value of the sequence. It is then possible to design the user client program so that it requests a renewal of its authentication parameters on a regular basis (every hour, every twelve hours,...). The client program can also choose a random number between 1 and the current sequence number, and require a renewal when the sequence number reaches the random number. These techniques would constitute a good

protection against race attacks, because they prevent an attacker

from accumulating data on the sequences of OTP’s he may see.

7. IANA Considerations

This document has no actions for IANA.

8. References

[0] Haller, N., "A One-Time Password System", RFC 2289, February 1998, <http://www.rfc-editor.org/info/rfc2289>.

[1] Rivest, R., "The MD4 Message-Digest Algorithm", RFC 1320, April 1992, <http://www.rfc-editor.org/info/rfc1320>.

[2] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992, <http://www.rfc-editor.org/info/rfc1321>.

[3] National Institute of Standards and Technology, NIST, "Announcing the Secure Hash Standard", FIPS 180-4, April 1995, <https://csrc.nist.gov/pubs/fips/180-4/final>.

[4] Eastlake, D., Hansen, T., "US Secure Hash Algorithms", RFC 6234, May 2011, <http://www.rfc-editor.org/info/rfc6234>.

Appendix A - OTP Verification Examples

This appendix provides a series of inputs and correct outputs for all three of the new OTP cryptographic hashes, specifically SHA256, SHA384 and SHA512. This document is intended to be used by developers for interoperability checks when creating generators or servers. Output is provided in both hexadecimal notation and the six-word encoding with the RFC2289 Standard Dictionary.

SHA256 ENCODINGS

Passphrase	Seed	Cnt	Hex	Six Word Format
This is a test.	TeSt	0	6FF2 6FCA 1D41 2482	DATA HANG USER SAP EVE TOM
This is a test.	TeSt	1	61A3 30FB 5460 EFE8	BUSY HAY SUP KYLE DO VEND
This is a test.	TeSt	99	A759 47C5 CB99 C0FE	KLAN OVAL TURN HERO HUFF FERN
AbCdEfGhIjK	alpha1	0	33B7 C6B4 7704 4BC2	PI MONK LENT TOOT WEB SODA
AbCdEfGhIjK	alpha1	1	9D7B 7E17 5E8D 0112	HUSH SIGN FOWL MOAN RINK GARY
AbCdEfGhIjK	alpha1	99	3CCC F2F5 054F 0E7C	SKY CLAY MOCK CAP TUNA SUB
OTP’s are good	correct	0	3ACF A072 7DE5 CAFA	SAW FAIL HUH WILL BOOM FAIR
OTP’s are good	correct	1	4013 9EB6 13CA 6C66	TEN HUNT LEST MAW KING PEP
OTP’s are good	correct	99	A194 AD13 0170 DF76	JILL KATE WED APT DEN MILL

SHA384 ENCODINGS

Passphrase	Seed	Cnt	Hex	Six Word Format
This is a test.	TeSt	0	A25E 045C 7326 E83A	JOEL TROY GIL SWAY DALE IDA
This is a test.	TeSt	1	0F19 0252 ACE0 9271	DOE OLIN HATH BLUE BUM ROW
This is a test.	TeSt	99	BE65 531C A0CC E0D5	MOOD NAG OHIO TON REEK COOL
AbCdEfGhIjK	alpha1	0	C542 1287 DBD0 6FFA	NONE EAT JOAN MARS BEN WONT
AbCdEfGhIjK	alpha1	1	4A3D 9E8A C1CA DF58	AIRY TOGO JOIN FOAM LICE LEEK
AbCdEfGhIjK	alpha1	99	8012 50DA 1475 F556	FILE HAIR RAT MOB BROW LATE
OTP’s are good	correct	0	3111 133B 8359 9CFA	OWL GALA REST BEE HOLT FAIL
OTP’s are good	correct	1	1D33 F015 80C0 F50D	IDA ISLE BAD ALP DON FROG
OTP’s are good	correct	99	F4D5 13BA 5694 3100	VICE KURD TOUR LEON UP FIND

SHA512 ENCODINGS

Passphrase	Seed	Cnt	Hex	Six Word Format
This is a test.	TeSt	0	9A33 631B AA8E 1097	HONK HOST OBOE BEAU SOAK ALTO
This is a test.	TeSt	1	72B2 58A6 8686 BC04	DIAL HALF MOT DAD COWL ANT
This is a test.	TeSt	99	41B5 690A 77B8 C1CC	TOO LAVA TUM TREK GIST SWAN

```
AbCdEfGhIjK     alpha1   0  40EA E6E7 F6DA 6A1F
                                          TIP BETH MELT TONY KIND DUB
AbCdEfGhIjK     alpha1   1  D53A DF93 1E55 FB53
                                          RUTH SARA SUIT SKI BUFF LAMB
AbCdEfGhIjK     alpha1  99  91DC 3DF2 5AE1 A17F
                                          GWEN SOLD EYED MAGI HER MOVE
OTP’s are good  correct  0  0F78 A93E 448A AC9A
                                          DOT NONE AVID GAME LASS ANNE
OTP’s are good  correct  1  208A CD3F 2C54 BB0E
                                          JOB BERG AVON BITS ALUM FUNK
OTP’s are good  correct 99  16AF FE29 10EC AB94
                                          GEM FIGS GEAR KEY OWNS OUTS
```


Appendix B - French Alternate Dictionary

This dictionary is made up of 2048 French words. None of these words appears in the RFC2289 Standard Dictionary, and none of these words are composed solely of A to F letters (thus avoiding confusing with hexadecimal numbers). This French dictionary MAY be used as an alternate dictionary by a user, although 35% of its words share at least two equal (alg(W)%2048) values (see appendix C below). But, once again, this list can be used straightforward as an alternate dictionary because, when receiving a set of six words from this list computed by the user willing to authenticate, the server just computes (alg(W)%2048) for each of the six words. It doesn’t care about the number of words in the alternate dictionary that generate the same (alg(W)%2048) value, nor does it need to know the alternate dictionary at all (as stated in RFC2289).

```
{ "AAS",   "ADO",   "AGA",   "AGE",   "AGI",   "AIE",   "AIL",   "AIS",
  "AIT",   "ALE",   "ALU",   "AME",   "AMI",   "ANE",   "ANS",   "API",
  "ARA",   "ARS",   "ASA",   "ASE",   "AUX",   "AXA",   "AXE",   "AYS",
  "BAI",   "BAL",   "BAS",   "BAU",   "BEL",   "BER",   "BIC",   "BIO",
```

```
  "BIP",   "BIS",   "BLE",   "BOA",   "BOF",   "BOL",   "BOT",   "BOX",
  "BRU",   "BUE",   "CAS",   "CEP",   "CES",   "CET",   "CHU",   "CIF",
  "CIL",   "CIS",   "CLE",   "COB",   "COI",   "COQ",   "COR",   "COU",
  "CRE",   "CRI",   "CRU",   "CUL",   "DAL",   "DAO",   "DAW",   "DER",
  "DEY",   "DIA",   "DIS",   "DIT",   "DIX",   "DOC",   "DOL",   "DOM",
  "DOP",   "DOS",   "DRU",   "DUC",   "DUO",   "DUR",   "DUS",   "DUT",
  "EAU",   "ECO",   "ECU",   "ELU",   "EMU",   "EON",   "EPI",   "ERE",
  "ERG",   "ERS",   "ETA",   "ETE",   "EUE",   "EUH",   "EUS",   "EUT",
  "EUX",   "EXO",   "FAQ",   "FAX",   "FER",   "FEU",   "FEZ",   "FIA",
  "FIC",   "FIE",   "FIL",   "FIS",   "FLA",   "FOB",   "FOC",   "FOI",
  "FOL",   "FOU",   "FOX",   "FUI",   "FUS",   "FUT",   "GAI",   "GAN",
  "GAZ",   "GEO",   "GEX",   "GIS",   "GIT",   "GLU",   "GOI",   "GON",
  "GOS",   "GOY",   "GRE",   "GUE",   "GUI",   "GUR",   "HAI",   "HEP",
  "HEU",   "HIA",   "HIC",   "HIE",   "HOU",   "HUA",   "HUI",   "HUN",
  "IBN",   "IBO",   "ICI",   "IDE",   "IFS",   "ILE",   "ILS",   "IPE",
  "ISO",   "IVE",   "IXA",   "IXE",   "JAS",   "JEU",   "JUS",   "KAN",
  "KAS",   "KEA",   "KHI",   "KIF",   "KIL",   "KIP",   "KIR",   "KOB",
  "KOP",   "KOT",   "KRU",   "KSI",   "KWA",   "KYU",   "LAI",   "LAO",
  "LAS",   "LEI",   "LEK",   "LEM",   "LES",   "LEU",   "LEV",   "LEZ",
  "LIA",   "LIS",   "LOF",   "LOI",   "LUE",   "LUI",   "LUS",   "LUT",
  "LUX",   "LYS",   "MAI",   "MAL",   "MAS",   "MAX",   "MEC",   "MEO",
  "MER",   "MES",   "MIE",   "MIL",   "MIR",   "MIS",   "MIX",   "MMM",
  "MOA",   "MOI",   "MOL",   "MON",   "MOR",   "MOU",   "MOX",   "MUA",
  "MUE",   "MUR",   "MUS",   "MUT",   "MYE",   "NEF",   "NEM",   "NEO",
  "NES",   "NEY",   "NEZ",   "NIA",   "NID",   "NIE",   "NIF",   "NOM",
  "NOS",   "NUA",   "NUE",   "NUI",   "NUL",   "NUS",   "OBA",   "OBI",
  "OHE",   "OHM",   "OIE",   "OKA",   "OLA",   "OLE",   "ONC",   "ONT",
```



```
  "OPE",   "ORS",   "OSA",   "OSE",   "OST",   "OTA",   "OTE",   "OUD",
  "OUF",   "OUH",   "OUI",   "OVE",   "OXO",   "OYE",   "PAF",   "PAS",
  "PEC",   "PEU",   "PFF",   "PHO",   "PIC",   "PIF",   "PIS",   "PIU",
  "PLI",   "PLU",   "POU",   "PRE",   "PSI",   "PST",   "PSY",   "PUA",
  "PUE",   "PUR",   "PUS",   "PUY",   "QAT",   "QIN",   "QUE",   "QUI",
  "RAB",   "RAC",   "RAD",   "RAI",   "RAS",   "RAZ",   "REA",   "REE",
  "REG",   "REM",   "REZ",   "RHE",   "RHO",   "RIA",   "RIE",   "RIF",
  "RIS",   "RIT",   "RIZ",   "ROC",   "ROI",   "ROM",   "ROS",   "RUA",
  "RUS",   "RUT",   "RUZ",   "SAI",   "SAR",   "SAS",   "SAX",   "SEL",
  "SEP",   "SES",   "SIC",   "SIL",   "SIX",   "SKA",   "SOC",   "SOI",
  "SOL",   "SOM",   "SOT",   "SOU",   "SPI",   "SUA",   "SUC",   "SUR",
  "SUS",   "SUT",   "TAC",   "TAF",   "TAO",   "TAS",   "TAT",   "TAU",
  "TEC",   "TEK",   "TEL",   "TEP",   "TER",   "TES",   "TET",   "TEX",
  "TIF",   "TIR",   "TOC",   "TOI",   "TOT",   "TRI",   "TUA",   "TUE",
  "TUF",   "TUS",   "TUT",   "UNE",   "UNI",   "UNS",   "URE",   "USA",
  "UTE",   "VAL",   "VAR",   "VAS",   "VAU",   "VER",   "VES",   "VIA",
  "VIF",   "VIL",   "VIN",   "VIS",   "VIT",   "VOL",   "VOS",   "VUE",
  "VUS",   "WAP",   "WAX",   "WUS",   "XENON", "YAK",   "YEN",   "YIN",
  "YOD",   "YUE",   "ZEC",   "ZEE",   "ZEF",   "ZEK",   "ZEN",   "ZIG",
  "ZIP",   "ZOB",   "ZOE",   "ZOO",   "ZOU",   "ZUP",   "ZUT",
  "ABAT",  "ABER",  "ABOI",  "ABOT",  "ABRI",  "ABUS",  "ACCU",  "ACES",
  "ACNE",  "ACON",  "ACRA",  "ACTE",  "ACTU",  "ACUL",  "ADAS",  "ADAV",
  "ADNE",  "ADON",  "ADOS",  "AERA",  "AERE",  "AFAT",  "AFIN",  "AGAS",
  "AGES",  "AGHA",  "AGIE",  "AGIO",  "AGIR",  "AGIS",  "AGIT",  "AGUI",
  "AHAN",  "AIES",  "AIGU",  "AILE",  "AILS",  "AIMA",  "AIME",  "AINE",
  "AIRA",  "AIRE",  "AIRS",  "AISE",  "AISY",  "AJUT",  "AKAN",  "ALEA",
  "ALEM",  "ALES",  "ALFA",  "ALLA",  "ALLE",  "ALLO",  "ALOI",  "ALPE",
  "ALUN",  "ALUS",  "ALYA",  "AMAN",  "AMAS",  "AMER",  "AMIE",  "AMIS",
  "AMMI",  "AMUI",  "ANAL",  "ANAR",  "ANAS",  "ANEE",  "ANEL",  "ANES",
  "ANGE",  "ANIL",  "ANIS",  "ANON",  "ANSE",  "ANUS",  "AOUT",  "APAX",
```

```
  "APEX",  "APIS",  "APRE",  "APTE",  "ARAC",  "ARAK",  "ARAS",  "ARCS",
  "ARDU",  "AREC",  "AREG",  "ARES",  "AREU",  "ARIA",  "ARMA",  "ARME",
  "AROL",  "ARUM",  "ASES",  "ASIN",  "ASPE",  "ASPI",  "ASSE",  "ASTI",
  "ATRE",  "AUBE",  "AUGE",  "AULA",  "AULX",  "AUNA",  "AUNE",  "AVAL",
  "AVEC",  "AVEN",  "AVEU",  "AVEZ",  "AXAI",  "AXAS",  "AXAT",  "AXEE",
  "AXEL",  "AXER",  "AXES",  "AXEZ",  "AXIS",  "AYEZ",  "AZUR",  "BACS",
  "BAES",  "BAHT",  "BAIE",  "BAIN",  "BAIS",  "BALS",  "BANC",  "BANI",
  "BANS",  "BARS",  "BASA",  "BASI",  "BATA",  "BATI",  "BATS",  "BAUD",
  "BAUX",  "BAVA",  "BAVE",  "BAYA",  "BAYE",  "BEAI",  "BEAS",  "BECS",
  "BEES",  "BEEZ",  "BEGU",  "BEKE",  "BELE",  "BELS",  "BENE",  "BENI",
  "BENS",  "BERK",  "BERS",  "BETE",  "BEUR",  "BEYS",  "BIBI",  "BICS",
  "BIEF",  "BIGE",  "BILA",  "BINA",  "BINE",  "BINZ",  "BIOS",  "BIPA",
  "BIPE",  "BIPS",  "BIRR",  "BISA",  "BISE",  "BITA",  "BITU",  "BIWA",
  "BLES",  "BLET",  "BLEU",  "BLOG",  "BOAS",  "BOBO",  "BOBS",  "BOER",
  "BOGE",  "BOGS",  "BOIS",  "BOIT",  "BOLS",  "BOME",  "BONI",  "BONS",
  "BOPS",  "BORA",  "BORD",  "BORT",  "BOTE",  "BOTS",  "BOUC",  "BOUE",
  "BOUH",  "BOUM",  "BOUR",  "BOUS",  "BOXA",  "BOXE",  "BOYS",  "BRAI",
```



```
  "BRAS",  "BREF",  "BREN",  "BRIE",  "BRIK",  "BRIN",  "BRIO",  "BRIS",
  "BROC",  "BROL",  "BROU",  "BRRR",  "BRUI",  "BRUN",  "BRUS",  "BRUT",
  "BUEE",  "BUES",  "BUGS",  "BUIS",  "BUNA",  "BUNS",  "BURE",  "BUSA",
  "BUSC",  "BUSE",  "BUTA",  "BUTE",  "BUTO",  "BUTS",  "CABS",  "CADI",
  "CAGE",  "CAID",  "CALA",  "CALE",  "CALO",  "CALS",  "CAMA",  "CAMP",
  "CANA",  "CAPA",  "CAPE",  "CAPO",  "CAPS",  "CARI",  "CARS",  "CARY",
  "CASA",  "CATA",  "CATI",  "CAVA",  "CAYE",  "CECI",  "CEDI",  "CELA",
  "CELE",  "CENE",  "CENS",  "CEPE",  "CEPS",  "CERF",  "CERS",  "CEUX",
  "CHAH",  "CHAI",  "CHAN",  "CHAS",  "CHEB",  "CHER",  "CHEZ",  "CHIA",
  "CHIE",  "CHIP",  "CHOC",  "CHOP",  "CHTI",  "CHUE",  "CHUS",  "CHUT",
  "CHVA",  "CIAO",  "CIEL",  "CILS",  "CIME",  "CINE",  "CINQ",  "CIRA",
  "CIRE",  "CITA",  "CIVE",  "CLAC",  "CLAP",  "CLEF",  "CLES",  "CLIC",
  "CLIM",  "CLIN",  "CLIP",  "CLOS",  "CLOU",  "COBS",  "COCU",  "COEF",
  "COIR",  "COIS",  "COIT",  "COLO",  "COLS",  "CONE",  "CONS",  "COPS",
  "COQS",  "CORS",  "COSY",  "COTA",  "COTE",  "COTI",  "COUD",  "COUP",
  "COUR",  "COUS",  "COUT",  "CRAC",  "CRAN",  "CRAU",  "CREA",  "CREE",
  "CRET",  "CRIA",  "CRIC",  "CRIE",  "CRIN",  "CRIS",  "CROC",  "CRUE",
  "CRUS",  "CRUT",  "CUBI",  "CUCU",  "CUIR",  "CUIS",  "CUIT",  "CULA",
  "CULE",  "CULS",  "CURA",  "CUTI",  "CUVA",  "CUVE",  "CYAN",  "CYME",
  "CYON",  "CZAR",  "DABS",  "DAHU",  "DAIL",  "DAIM",  "DAIS",  "DAMA",
  "DAME",  "DAMS",  "DANS",  "DAOS",  "DARD",  "DARI",  "DAUW",  "DAWS",
  "DEBS",  "DECI",  "DECO",  "DECU",  "DEFI",  "DEJA",  "DELA",  "DEME",
  "DEMI",  "DEMO",  "DENI",  "DENT",  "DERS",  "DEUG",  "DEUX",  "DEYS",
  "DIAM",  "DIAS",  "DIBI",  "DICO",  "DIEU",  "DINA",  "DIOL",  "DIOT",
  "DIRA",  "DISE",  "DITE",  "DITO",  "DITS",  "DIVA",  "DOCS",  "DODO",
  "DODU",  "DOGE",  "DOIS",  "DOIT",  "DOJO",  "DOLA",  "DOLO",  "DOLS",
  "DOMS",  "DONA",  "DONC",  "DONF",  "DONG",  "DONS",  "DONT",  "DOPA",
  "DOPE",  "DOPS",  "DORE",  "DORS",  "DORT",  "DOSA",  "DOTA",  "DOTS",
  "DOUA",  "DOUE",  "DOUM",  "DOUX",  "DRAP",  "DROP",  "DRUE",  "DRUS",
  "DRYS",  "DUBS",  "DUCE",  "DUCS",  "DUES",  "DUIT",  "DUOS",  "DUPA",
  "DUPE",  "DURA",  "DURE",  "DURS",  "DYKE",  "DYNE",  "EAUX",  "EBAT",
  "ECHA",  "ECHE",  "ECHU",  "ECOS",  "ECOT",  "ECRU",  "ECUS",  "EDAM",
  "EGAL",  "EJET",  "ELFE",  "ELIA",  "ELIE",  "ELIS",  "ELIT",  "ELLE",
  "ELUA",  "ELUE",  "ELUS",  "ELUT",  "EMBU",  "EMET",  "EMEU",  "EMIA",
  "EMIE",  "EMIR",  "EMIS",  "EMOI",  "EMOU",  "EMUE",  "EMUS",  "EMUT",
  "ENOL",  "ENTA",  "ENTE",  "ENVI",  "EONS",  "EPAR",  "EPEE",  "EPIA",
  "EPIE",  "EPIS",  "EPOI",  "ERES",  "ERGS",  "ERRA",  "ERRE",  "ERSE",
  "ESSE",  "ESTE",  "ETAI",  "ETAL",  "ETAT",  "ETAU",  "ETES",  "ETOC",
  "ETRE",  "ETUI",  "EUES",  "EURO",  "EVOE",  "EWES",  "EXAM",  "EXIL",
  "EXIT",  "EXON",  "EXOS",  "EXPO",  "EYRA",  "FACS",  "FADO",  "FAFS",
```

```
  "FAIM",  "FAIS",  "FAIT",  "FAIX",  "FANA",  "FANE",  "FANS",  "FAON",
  "FAQS",  "FARD",  "FARE",  "FARO",  "FARS",  "FART",  "FATS",  "FAUT",
  "FAUX",  "FAXA",  "FAXE",  "FEAL",  "FEES",  "FELA",  "FELE",  "FERA",
  "FERS",  "FERU",  "FETA",  "FETE",  "FETU",  "FEUE",  "FEUJ",  "FEUS",
  "FEUX",  "FEVE",  "FIAI",  "FIAS",  "FIAT",  "FICS",  "FIEE",  "FIEL",
  "FIER",  "FIES",  "FIEU",  "FIEZ",  "FIFI",  "FIGE",  "FILA",  "FILO",
  "FILS",  "FINI",  "FINN",  "FINS",  "FION",  "FIQH",  "FISC",  "FIXA",
```



```
  "FIXE",  "FIZZ",  "FLAC",  "FLAN",  "FLET",  "FLIC",  "FLIP",  "FLOE",
  "FLOP",  "FLOT",  "FLOU",  "FLUA",  "FLUO",  "FLUX",  "FOCS",  "FOGS",
  "FOHN",  "FOIE",  "FOIN",  "FOIS",  "FORA",  "FORS",  "FOUI",  "FOUS",
  "FOUT",  "FOXE",  "FRAC",  "FRAI",  "FRIC",  "FRIS",  "FRIT",  "FROC",
  "FUGU",  "FUIE",  "FUIR",  "FUIS",  "FUIT",  "FUMA",  "FUNE",  "FUNS",
  "FUSA",  "FUTE",  "FUTS",  "GABA",  "GADE",  "GAGA",  "GAGS",  "GAIE",
  "GAIS",  "GALS",  "GANS",  "GANT",  "GAPS",  "GARA",  "GARE",  "GARI",
  "GARS",  "GATA",  "GAVA",  "GAYS",  "GAZA",  "GAZE",  "GEAI",  "GELA",
  "GELE",  "GELS",  "GEMI",  "GENA",  "GENS",  "GEOS",  "GERA",  "GERE",
  "GIGA",  "GINS",  "GITA",  "GITE",  "GLAS",  "GLEY",  "GLIE",  "GLUA",
  "GLUI",  "GLUS",  "GNON",  "GNOU",  "GOBA",  "GOBE",  "GODA",  "GODE",
  "GOGE",  "GOGO",  "GOIM",  "GOIS",  "GOND",  "GONS",  "GORD",  "GOTH",
  "GOUM",  "GOUR",  "GOYM",  "GOYS",  "GRAM",  "GRAS",  "GRAU",  "GREA",
  "GREC",  "GREE",  "GRES",  "GRIL",  "GRIP",  "GRIS",  "GROG",  "GROS",
  "GRRR",  "GRUE",  "GUAI",  "GUEA",  "GUEE",  "GUES",  "GUET",  "GUIB",
  "GUIS",  "GUNZ",  "GURS",  "GUSS",  "GYMS",  "HADJ",  "HAIE",  "HAIK",
  "HAIS",  "HAIT",  "HAJE",  "HAKA",  "HALA",  "HARO",  "HASE",  "HATA",
  "HAUT",  "HAVA",  "HAVI",  "HEIN",  "HELA",  "HELE",  "HEME",  "HEUR",
  "HIAI",  "HIAS",  "HIAT",  "HIEE",  "HIER",  "HIES",  "HIEZ",  "HIFI",
  "HILE",  "HITS",  "HOAX",  "HOCA",  "HOIR",  "HOLA",  "HOMO",  "HOPI",
  "HORA",  "HORS",  "HOTE",  "HOTS",  "HOTU",  "HOUA",  "HOUE",  "HOUP",
  "HOUX",  "HUAI",  "HUAS",  "HUAT",  "HUBS",  "HUEE",  "HUER",  "HUES",
  "HUEZ",  "HUIS",  "HUIT",  "HUMA",  "HUME",  "HUNE",  "HUNS",  "HURE",
  "HUTU",  "IBNS",  "IBOS",  "IDEE",  "IDEM",  "IDES",  "IGNE",  "IGUE",
  "IKAT",  "ILES",  "ILET",  "ILOT",  "IMAM",  "IMAN",  "IMBU",  "INDE",
  "INDU",  "INFO",  "INNE",  "INNU",  "INOX",  "INSU",  "INTI",  "INUK",
  "IODA",  "IODE",  "IPES",  "IRAI",  "IRAS",  "IRES",  "IREZ",  "ISBA",
  "ISSA",  "ISSU",  "ITOU",  "IULE",  "IVES",  "IVRE",  "IWAN",  "IXAI",
  "IXAS",  "IXAT",  "IXEE",  "IXER",  "IXES",  "IXEZ",  "IXIA",  "JABS",
  "JACO",  "JAIN",  "JAIS",  "JALE",  "JAMS",  "JANS",  "JARD",  "JARS",
  "JASA",  "JASE",  "JASS",  "JAZZ",  "JEEP",  "JETA",  "JETE",  "JETS",
  "JEUN",  "JEUX",  "JEZE",  "JOIE",  "JOJO",  "JOLI",  "JONC",  "JOTA",
  "JOUA",  "JOUE",  "JOUG",  "JOUI",  "JOUR",  "JUBE",  "JUGE",  "JUIF",
  "JUIN",  "JUMP",  "JUPE",  "JURA",  "JURE",  "JUTA",  "KADI",  "KAKI",
  "KALI",  "KAMI",  "KANA",  "KANS",  "KAON",  "KAPO",  "KART",  "KATA",
  "KAVA",  "KAWA",  "KAWI",  "KEAS",  "KEPI",  "KEUF",  "KEUM",  "KHAN",
  "KHAT",  "KHOL",  "KIDS",  "KIEF",  "KIFA",  "KIFE",  "KIFS",  "KIKI",
  "KILO",  "KILS",  "KILT",  "KINA",  "KINE",  "KIPS",  "KIRS",  "KITS",
  "KIWI",  "KOAN",  "KOBS",  "KOKA",  "KOLA",  "KOPS",  "KORA",  "KORE",
  "KOTA",  "KOTE",  "KOTO",  "KOTS",  "KRAK",  "KRUS",  "KSAR",  "KUNA",
  "KURU",  "KVAS",  "KWAS",  "KYAT",  "KYUS",  "LABO",  "LACA",  "LACS",
  "LADS",  "LAIC",  "LAIE",  "LAIS",  "LAIT",  "LAKH",  "LALA",  "LAMA",
  "LAOS",  "LAPA",  "LAPE",  "LAPS",  "LARE",  "LARI",  "LATS",  "LAVE",
  "LAYA",  "LAYE",  "LEGE",  "LEGO",  "LEGS",  "LEHM",  "LEKS",  "LEMS",
  "LESA",  "LESE",  "LEUR",  "LEUS",  "LEVA",  "LEVE",  "LEVS",  "LIAI",
  "LIAS",  "LIAT",  "MAAR",  "MACH",  "MACS",  "MAFE",  "MAGE",  "MAIA",
  "MAIE",  "MAIS",  "MAJE",  "MAKI",  "MALM",  "MALS",  "MAMY",  "MANS",
```

```
  "MANX",  "MAOS",  "MARA",  "MARI",  "MASO",  "MATA",  "MATI",  "MATS",
  "MATU",  "MAUX",  "MAXI",  "MAYA",  "MAYE",  "MAZA",  "MAZE",  "MECS",
  "MEDE",  "MEGA",  "MEGI",  "MELA",  "MELE",  "MELO",  "MELS",  "MEME",
  "MENA",  "MENE",  "MENS",  "MENT",  "MEOS",  "MERE",  "MERL",  "MERS",
  "MESA",  "META",  "METS",  "MEUF",  "MEUH",  "MEUS",  "MEUT",  "MEZE",
  "MIAM",  "MICA",  "MIDI",  "MIEL",  "MIEN",  "MIES",  "MILS",  "MIMA",
  "MIME",  "MINA",  "MING",  "MINS",  "MIPS",  "MIRA",  "MIRO",  "MIRS",
  "MISA",  "MISE",  "MISO",  "MITA",  "MIXA",  "MIXE",  "MOAI",  "MOAS",
  "MOBS",  "MOCO",  "MOHO",  "MOIE",  "MOIS",  "MOKA",  "MOKO",  "MOLY",
  "MOME",  "MONO",  "MONS",  "MORD",  "MORS",  "MOTO",  "MOTS",  "MOUD",
  "MOUE",  "MOUS",  "MOUT",  "MOXA",  "MOYA",  "MOYE",  "MUAI",  "MUAS",
  "MUAT",  "MUEE",  "MUER",  "MUES",  "MUET",  "MUEZ",  "MUGE",  "MUGI",
  "MUGS",  "MUID",  "MUNI",  "MUON",  "MURA",  "MURE",  "MURI",  "MURS",
  "MUSA",  "MUSC",  "MUSE",  "MUTA",  "MYES",  "NABI",  "NAFE",  "NAGA",
  "NAGE",  "NAGI",  "NAIF",  "NAIN",  "NAIS",  "NAIT",  "NAJA",  "NANA",
  "NAOS",  "NARD",  "NASE",  "NAYS",  "NAZE",  "NAZI",  "NEEM",  "NEES",
  "NEFS",  "NEMI",  "NEMS",  "NENE",  "NEOS",  "NEPE",  "NERE",  "NERF",
  "NETS",  "NEUF",  "NEVE",  "NEYS",  "NIAI",  "NIAS",  "NIAT",  "NIDA",
  "NIDS",  "NIEE",  "NIER",  "NIES",  "NIET",  "NIEZ",  "NIFE",  "NIFS",
  "NITS",  "NIVE",  "NIXE",  "NOCA",  "NOCE",  "NOIE",  "NOIR",  "NOIX",
  "NOME",  "NOMS",  "NORD",  "NORI",  "NOTA",  "NOUA",  "NOUC",  "NOUE",
  "NOUS",  "NOVE",  "NOVI",  "NOYA",  "NOYE",  "NUAI",  "NUAS",  "NUAT",
  "NUEE",  "NUER",  "NUES",  "NUEZ",  "NUIS",  "NUIT",  "NULS",  "OBAS",
  "OBEI",  "OBEL",  "OBIS",  "OBIT",  "OBUS",  "OCRA",  "OCRE",  "ODES",
  "OEIL",  "OEUF",  "OGAM",  "OGRE",  "OHMS",  "OIES",  "OING",  "OINS",
  "OKAS",  "OKRA",  "OLAS",  "OLIM",  "OLLE",  "OMET",  "OMIS",  "ONDE",
  "ONYX",  "ONZE",  "OPEN",  "OPES",  "OPTA",  "OPTE",  "OPUS",  "ORBE",
  "ORDI",  "ORDO",  "OREE",  "ORES",  "ORGE",  "ORIN",  "ORLE",  "ORME",
  "ORNA",  "ORNE",  "ORYX",  "OSAI",  "OSAS",  "OSAT",  "OSEE",  "OSER",
  "OSES",  "OSEZ",  "OSSU",  "OSTO",  "OSTS",  "OTAI",  "OTAS",  "OTAT",
  "OTEE",  "OTER",  "OTES",  "OTEZ",  "OUAH",  "OUDS",  "OUED",  "OUFS",
  "OUIE",  "OUIN",  "OUIR",  "OUIS",  "OUPS",  "OURS",  "OUZO",  "OVEE",
  "OVES",  "OVIN",  "OVNI",  "OXER",  "OYAT",  "OYES",  "OYEZ",  "PACA",
  "PACK",  "PACS",  "PAFS",  "PAGE",  "PAGI",  "PAIE",  "PAIN",  "PAIR",
  "PAIS",  "PAIT",  "PAIX",  "PALA",  "PALE",  "PALI",  "PALS",  "PALU",
  "PAMA",  "PAME",  "PANA",  "PANE",  "PANS",  "PAON",  "PAPA",  "PAPE",
  "PAPI",  "PAPY",  "PARA",  "PARC",  "PARE",  "PARI",  "PARS",  "PART",
  "PARU",  "PATE",  "PATI",  "PATS",  "PAVA",  "PAVE",  "PAYA",  "PAYE",
  "PAYS",  "PEAN",  "PEAU",  "PECS",  "PEDE",  "PELA",  "PELE",  "PEND",
  "PENE",  "PEON",  "PEPE",  "PEPS",  "PERD",  "PERE",  "PERF",  "PERI",
  "PERM",  "PERS",  "PESA",  "PESE",  "PESO",  "PETA",  "PETE",  "PETS",
  "PEUH",  "PEUL",  "PEUR",  "PEUT",  "PEUX",  "PEZE",  "PFFT",  "PFUT",
  "PHOS",  "PHOT",  "PIAF",  "PIAN",  "PICA",  "PICS",  "PIED",  "PIER",
  "PIES",  "PIEU",  "PIFA",  "PIFE",  "PIFS",  "PIGE",  "PILA",  "PILE",
  "PILS",  "PINE",  "PINS",  "PION",  "PIPA",  "PIPE",  "PIPI",  "PIPO",
  "PIRE",  "PISE",  "PITA",  "PITE",  "PIVE",  "PLAF",  "PLAN",  "PLAT",
  "PLIA",  "PLIE",  "PLIS",  "PLOC",  "PLOT",  "PLUS",  "PLUT",  "PNEU",
```



```
  "POCO",  "POGO",  "POIL",  "POIS",  "POIX",  "POLE",  "POLI",  "POLO",
  "POLY",  "POND",  "PONT",  "POOL",  "POPE",  "POPS",  "PORC",  "PORE",
  "PORT",  "POSA",  "POSE",  "POTE",  "POTS",  "POTU",  "POUF",  "POUH",
  "POUM",  "POUR",  "POUX",  "POYA",  "PRAO",  "PRES",  "PRET",  "PRIA",
```

```
  "PRIE",  "PRIS",  "PRIT",  "PRIX",  "PROF",  "PROS",  "PROU",  "PSYS",
  "PUAI",  "PUAS",  "PUAT",  "PUBS",  "PUCE",  "PUCK",  "PUEE",  "PUER",
  "PUES",  "PUEZ",  "PUIS",  "PUJA",  "PULA",  "PULL",  "PUMA",  "PUNA",
  "PUNI",  "PUNK",  "PUNT",  "PUPE",  "PURE",  "PURO",  "PURS",  "PUTE",
  "PUTS",  "PUTT",  "PUYS",  "QATS",  "QING",  "QINS",  "QUAI",  "QUEL",
  "QUIA",  "QUIZ",  "QUOI",  "RAAG",  "RABE",  "RABS",  "RACA",  "RADA",
  "RADE",  "RADS",  "RAGA",  "RAIA",  "RAIE",  "RAIS",  "RAIT",  "RAJA",
  "RAKI",  "RALA",  "RALE",  "RAMA",  "RAME",  "RAMI",  "RAND",  "RANG",
  "RANI",  "RANZ",  "RAPA",  "RAPE",  "RAPS",  "RAPT",  "RASA",  "RASE",
  "RATA",  "RATS",  "RAVI",  "RAYA",  "RAYE",  "REAC",  "REAI",  "REAS",
  "REAT",  "REBU",  "RECU",  "REDU",  "REER",  "REES",  "REEZ",  "REGI",
  "REGS",  "REIS",  "RELU",  "REMS",  "RENE",  "REPS",  "REPU",  "RETS",
  "REVA",  "REVE",  "REVU",  "RHES",  "RHUM",  "RIAD",  "RIAL",  "RIAS",
  "RIDA",  "RIEL",  "RIEN",  "RIES",  "RIEZ",  "RIFF",  "RIFS",  "RIMA",
  "RIOS",  "RIPA",  "RIPE",  "RIRA",  "RIRE",  "RISS",  "RITS",  "RIVA",
  "RIVE",  "RIXE",  "ROBA",  "ROBS",  "ROCS",  "RODA",  "ROIS",  "ROLE",
  "ROMS",  "ROND",  "ROSI",  "ROTA",  "ROTE",  "ROTI",  "ROTS",  "ROUA",
  "ROUE",  "ROUF",  "ROUI",  "ROUX",  "RUAI",  "RUAS",  "RUAT",  "RUEE",
  "RUER",  "RUES",  "RUEZ",  "RUGI",  "RUMB",  "RUNE",  "RUPA",  "RUPE",
  "RUSA",  "RUTS",  "RYAD",  "RYAL",  "RYES",  "SACS",  "SADO",  "SAGA",
  "SAIE",  "SAIN",  "SAIS",  "SAIT",  "SAKE",  "SAKI",  "SALA",  "SALI",
  "SALS",  "SAMU",  "SANA",  "SANS",  "SAPA",  "SAPE",  "SARI",  "SARS",
  "SART",  "SATE",  "SATI",  "SAUF",  "SAUR",  "SAUT",  "SAXE",  "SAXO",
  "SCIA",  "SCIE",  "SEAU",  "SECS",  "SECU",  "SEGA",  "SEIN",  "SELS",
  "SEMA",  "SEME",  "SENE",  "SENS",  "SEPS",  "SEPT",  "SERA",  "SERE",
  "SERF",  "SERS",  "SERT",  "SEUL",  "SEVE",  "SEVI",  "SEXE",  "SEXY",
  "SHAH",  "SHIT",  "SIAL",  "SIDA",  "SIDI",  "TAAL",  "TACO",  "TACS",
  "TAEL",  "TAFS",  "TAGS",  "TAIE",  "TAIN",  "TAIS",  "TAIT",  "TAKA",
  "TALA",  "TALC",  "TANS",  "TANT",  "TAON",  "TAOS",  "TAPA",  "TAPE",
  "TAPI",  "TARA",  "TARD",  "TARE",  "TARI",  "TARO",  "TARS",  "TAUX",
  "TAXA",  "TAXE",  "TAXI",  "TEST",  "TOUS",  "TRES",  "TROP",  "TRIO",
  "TRUC",  "TUBE",  "UNIR",  "VERS",  "VERT",  "VELO",  "VITE",  "VLAN",
  "VOIR",  "VOIX",  "VOUS",  "VRAI",  "WOLF",  "XENON",  "YACK", "YEUX",
  "YOGA",  "ZINC"
};
```


Appendix C - Statistical analysis of EN and FR dictionaries

For a given dictionary (EN or FR) and a given hash algorithm (md5, sha1, sha256, sha384 or sha512), this table shows the number (and ratio on 2048 words) of collisions - that is, the number of words that share at least two equal (alg(word) % 2048) values.

The EN dictionary is the RFC2289 standard, while the FR dictionary is made of 2048 French different words shown in Appendix B above. None of these words appears in the English RFC2289 standard dictionary.

\ alg	MD5	SHA1	SHA256	SHA384	SHA512

lang \					
FR	759 37,0%	766 37,4%	757 37,0%	763 37,3%	764 37,3%
EN	727 35,5%	722 35,3%	730 35,6%	762 37,2%	755 36,9%

These figures show that collision rate varies from 35,3% to 37,4%, which can be considered very high, whatever the dictionary, word distribution and hash algorithm. They mean that, among 10 words randomly chosen in a source dictionary, almost 4 of them share 1 slot in the final (computed) alternate dictionary.

Author’s Address
Regis Corbel
Orange Group
2 avenue Pierre Marzin
22300 Lannion
FRANCE
regis.corbel@orange.com