Number Codes
KPH January 2024 Event

Dave, KA8VHF
Dick, N0UC

Introduction

- **Maritime Radio Historical Society**
  - The Maritime Radio Historical Society (MRHS) was formed on 12 July 1999, the date of the supposed last commercial Morse transmission in the US.
  - www.radiomarine.org

- **KPH** is a coast radio station on the Pacific Coast of the United States. For most of the 20th century, it provided ship to shore communications including telegrams and marine telex service. The station discontinued commercial operation in 1998 but is operated occasionally as a historic service – its signal can be received over a large portion of the western hemisphere. – *Wikipedia*

- **KPH** has returned to the air in addition to **KSM**, **KFS** and **K6KPH** operated by MRHS.

- The Maritime Radio Historical Society is composed of a small group of dedicated individuals committed to the restoration and preservation of the artifacts of our maritime radio history with special emphasis on the US West Coast. – *Facebook*

KPH Event on January 20, 2024

- Radio Station KPH transmitted a Numbers Message via CW and RTTY at the appointed date/time of 20-JAN-2024 2100z (300p CST).

- CW transmission repeated the Numbers Message twice by hand at approximately 13-15 wpm. Given the length of the message, the transmission was approximately 5 minutes long (each).

- RTTY transmission followed, repeating the message four times.

- <u>Mission Critical Materials</u>
  - One Time Pad (OTP)
  - Conversion Chart
  - Code Book

CQ CQ CQ DE KPH KPH KPH
CQ CQ CQ DE KPH KPH KPH
NUMBERS MESSAGE FOLLOWS
=
447 447 447
=
14408 22398 89277 37674 58289
07722 15378 84975 30552 61128
69986 02108 68467 10079 92331
32982 54092 37446 22905 15340
17129 81152 39418 67073 25414
81456 43361
=

Mission Critical Materials - OTP

- **One Time Pad (OTP)** – a table of 5-digit groups. Once aligned properly to the encoded message (also in 5-digit groups), these values are lined up and added *modulo 10* to arrive at the resultant decoded set of numbers.

Mission Critical Materials - OTP

One-Time Pad OTP

The unbreakable code

The **One-Time Pad**, or **OTP** is an encryption technique in which each character of the plaintext is combined with a character from a random *key stream*. Originally described in 1882 by banker Frank Miller (USA), it was re-invented in 1917 by Gilbert Vernam and Joseph Mauborgne. When applied correctly, the OTP provides a truely unbreakable cipher. It is named after the sheets of paper (pads) on which the key stream was usually printed. It also exists as *One Time Tape* (OTT).

The image on the right shows a typical OTP booklet as it was used by agents of the former Soviet Union (USSR) during the 1960s. It consists of a stack of small very thin pages, each with a series of random 5-digit numbers on them. Each page was destroyed immediately after use.

OTPs like this, were commonly used for sending coded messages via a Russian spy radio set such as the R-353, often in relation to the mysterious Numbers Stations on the short wave radio bands. The OTP booklet shown here is from the internal collection of the Dutch Intelligence Agency AIVD.

In this section, we shows a selection of OTP systems from a variety of sources and countries. Although the exact operating procedure varies between OTP systems, we will try to give examples whenever possible. Real OTP booklets are extremely rare as they were normally destroyed after use. The ones that did survive are generally in the hands of the intelligence and law enforcement agencies that used or confiscated them. Click any of the thumbnails below for further details.

Mission Critical Materials - OTP

R-394K   Strizh K

Analogue spy radio set with burst encoder · USSR

R-394K and **R-394D**, codenamed **Strizh-K** and **Strizh-D** (Russian: Стриж), [1] are self-contained short wave (SW) radio sets for clandestine operations, also known as spy radio sets, developed around 1975 in the former Soviet Union (USSR) as the successor to earlier radio sets like the R-353 and R-354. They were intended for use by Special Forces (SF) and for agent communication, by services like the KGB and GRU. It features an analogue PLL and a built-in analogue or digital burst encoder. In 1983, the R-394(K/D) was succeeded by the all-digital R-394KM and R-394T.

The modular radio is housed in a watertight metal carrying case – similar to that of the later R-394KM – and is powered by an internal 12V battery. The transmitter uses an analogue phase-locked loop (PLL) and can be adjusted between 1.5 and 13.5 MHz in 1 kHz steps.

The crystal-controlled receiver has 190 fixed channels and an always-on beat frequency oscillator (BFO) for the reception of CW signals. At the far left is the high-speed burst encoder. Accessories like headphones, screwdriver, spare fuses and light bulbs are stowed in the top lid.

At least two different versions of the R-394K are known, both of which are extremely rare. The oldest one has an analogue burst encoder that uses magnetic tape, whilst a later one has a digital burst encoder. The latter is shown above and was short-lived. It can be seen as an intermediate step towards the design of the fully digital military R-394KM and the R-394T agent version.

Mission Critical Materials

- **Conversion Chart** – used to convert decoded numbers into letters, numbers punctuation, and symbols.

CODE	A	E	I	N	O	T	Conversion Chart № 03086		
0	1	2	3	4	5	6			
B	C	D	F	G	H	J	K	L	M
70	71	72	73	74	75	76	77	78	79
P	Q	R	S	U	V	W	X	Y	Z
80	81	82	83	84	85	86	87	88	89
FIG	(.)	(:)	(')	(,)	(+)	(-)	(=)	REQ	SPC
90	91	92	93	94	95	96	97	98	99
0	1	2	3	4	5	6	7	8	9
000	111	222	333	444	555	666	777	888	999

Mission Critical Materials

- **Code Book** –a list used to convert common words and phrases to 3-digit numbers.

- It contained various words/phrases that would normally require more than four digits to convert.

- The use of a codebook is optional but can reduce a message length and transmission time considerably.

- The 3-digit codes are non-consecutive values and are carefully chosen in order to detect single-digit errors and in most cases double-digit errors during decryption.

CODE BOOK #733

000 ABORT	253 DECODE	505 MILITARY	758 STREET
019 ACCEPT	262 DELAY	514 MONEY	767 SUBWAY
028 ACCESS	271 DIFFICULT	523 MONTH	776 SUCCESS
037 ADDRESS	280 DOCUMENT	532 MORNING	785 SUPPLY
046 AFFIRMATIVE	299 ENCODE	541 MORSE	794 SUPPORT
055 AGENT	307 EVENING	550 NEGATIVE	802 TELEPHONE
064 AIRPLANE	316 EXECUTE	569 NIGHT	811 TODAY
073 AIRPORT	325 FACTORY	578 OBSERVATION	820 TOMORROW
082 ANSWER	334 FAILED	587 PASSPORT	839 TRAIN
091 AUTHORITY	343 FERRY	596 PERSON	848 TRANSFER
109 BETWEEN	352 FLIGHT	604 PHOTOGRAPH	857 TRANSMIT
118 BORDER	361 FREQUENCY	613 POSITIVE	866 TRAVEL
127 BUILDING	370 HARBOUR	622 POSSIBLE	875 TRUCK
136 CANCEL	389 HELICOPTER	631 POWER	884 UNABLE TO
145 CHANGE	398 HIGHWAY	640 PRIORITY	893 URGENT
154 CIVILIAN	406 IDENTITY	659 PROBLEM	901 VERIFY
163 COMPROMISE	415 IMMEDIATE	668 QUESTION	910 WEEK
172 COMPUTER	424 IMPOSSIBLE	677 RADIO	929 WITHIN
181 CONFIRM	433 INFORMATION	686 RECEIVE	938 YESTERDAY
190 CONTACT	442 INSTRUCTIONS	695 RENDEZVOUS	947 MOSCOW
208 COORDINATE	451 LOCATE	703 REPEAT	956 BERLIN
217 COUNTRY	460 LOCATION	712 RESERVATION	965 PARIS
226 COVERT	479 MAIL	721 ROUTINE	974 LONDON
235 CURRENT	488 MEETING	730 SATELLITE	983 ISTANBUL
244 DANGER	497 MESSAGE	749 SHIP	992 PRAGUE

Encoding / Decoding

- **Required items: OTP, Conversion Chart, Codebook**
- **Encoding**
  - **The Conversion Chart converts text to numbers**
  - **The Code Book converts common words text longer than 3 or 4 characters to numbers**
  - **The OTP is used to encrypt the numbers. These numbers are assembled into 5-digit groups.**
- **Decoding**
  - **The OTP is used to decrypt the numbers according to the rules.**
  - **The Conversion Chart converts the numbers to text.**
  - **The Code Book converts three-digit code to the mapped word.**

Decoding Rules

- **Step 1 – Identify Message Key Indicator / Start of Message**
  - **The first 5-digit group in the Message is the Key Indicator**
  - **Find the Key Indicator in the OTP.**
  - **The Message begins with the 5-digit group <u>following</u> the Key Indicator (i.e. the 2nd 5-digit block)**

| 8 5 8 3 3 | | 5 7 2 7 2 | 1 7 4 4 2 | 4 6 9 4 0 | 3 2 5 6 1 |

Decoding Rules

- **Step 2 – Decrypt the message**
    - **Write the OTP numbers underneath the Message numbers starting with the Key Indicator**
    - **Add the OTP digits to the Message digits, digit by digit, from left to right.**
    - **The addition is performed *modulo 10*, i.e. without carrying.**
    - **Examples:**
        - **5 + 9 = 4 (not 14, drop the 1)**
        - **8 + 4 = 2 (not 12, drop the 1)**
        - **3 + 6 = 9**

8	5	8	3	3		5	7	2	7	2		1	7	4	4	2		4	6	9	4	0		3	2	5	6	1
8	5	8	3	3		2	7	3	8	5		1	2	5	3	6		4	8	8	7	7		4	7	6	3	0
K	E	Y	I	D		7	4	5	5	7		2	9	9	7	8		8	4	7	1	7		7	9	1	9	1

Decoding Rules

- **Step 3 – Convert decoded numbers to text using Conversation Chart (CC)**
  - **There are single-digit and double-digit values to consider.**
  - **If the first/next digit is 1-6, it represents a single-digit value (CC row 1)**
  - **If the first/next digit is 7, 8, or 9, it represents a double-digit value (CC rows 2, 3, 4)**
  - **If the first/next digit is a 0 (CODE), it will be followed by a three-digit code that represents a word or expression from the Code Book.**
  - **Numbers are preceded by 90 (FIG), repeated three times, then ended with 90 (FIG).**
  - **Spaces may be omitted if it does not impact the message readability.**
  - **Where needed, 91 (.) or 0 (CODE) is used to fully pad the last 5-digit block.**

8	5	8	3	3		5	7	2	7	2		1	7	4	4	2		4	6	9	4	0		3	2	5	6	1
8	5	8	3	3		2	7	3	8	5		1	2	5	3	6		4	8	8	7	7		4	7	6	3	0
K	E	Y	I	D		7	4	5	5	7	2	9	9	7	8		8	4	7	1	7	7	9	1	9	1
						G		O	O	D		SPC		L			U		C		K		.		.	

Decoding Rules

- **Step 4 – Assemble final message**
  - **Literal translated message: GOOD SPC LUCK..**
  - **Final readable message: GOOD LUCK**

8	5	8	3	3		5	7	2	7	2		1	7	4	4	2		4	6	9	4	0		3	2	5	6	1
8	5	8	3	3		2	7	3	8	5		1	2	5	3	6		4	8	8	7	7		4	7	6	3	0
K	E	Y	I	D		7	4	5	5	7	2	9	9	7	8		8	4	7	1	7	7	9	1	9	1
						G		O	O	D		SPC		L			U		C		K		.		.	

Your First Message!

85833 58993 66063 48715 31190

Your First Message! (Solution)

85833 58993 66063 48715 31190

8	5	8	3	3		5	8	9	9	3		6	6	0	6	3		4	8	7	1	5		3	1	1	9	0
8	5	8	3	3		2	7	3	8	5		1	2	5	3	6		4	8	8	7	7		4	7	6	3	0
K	E	Y	I	D		7	5	2	7	8		7	8	5	9	9		8	6	5	8	2		7	8	7	2	0
							H		E	L			L		O	SPC			W		O	R			L		D	0

Decoded Characters from Conversion Chart
HELLO SPC WORLD 0

Readable Message
HELLO WORLD

Message #2

85833 53914 71312 84129 12342
78949 98891 47419 51169 82471

Message #2 (Solution)

85833 53914 71312 84129 12342

78949 98891 47419 51169 82471

8	5	8	3	3		5	3	9	1	4		7	1	3	1	2		8	4	1	2	9		1	2	3	4	2
8	5	8	3	3		2	7	3	8	5		1	2	5	3	6		4	8	8	7	7		4	7	6	3	0
K	E	Y	I	D		7	0	2	9	9		8	3	8	4	8	2	2	9	9	6		5	9	9	7	2
						B		E	SPC			S		U		R		E	SPC		T		O	SPC		D

7	8	9	4	9		9	8	8	9	1		4	7	4	1	9		5	1	1	6	9		8	2	4	7	1
1	4	4	0	8		8	0	0	6	7		0	1	8	4	9		0	0	6	2	7		5	2	8	2	0
8	2	3	4	7	7	8	8	5	8	4	8	2	5	8	5	1	7	8	6	3	4	2	9	1
R	I	N	K		Y	O	U	R	O	V	A	L	T	I	N	E	.

Decoded Characters from Conversion Chart

BE SPC SURE SPC TO SPC DRINKYOUROVALTINE.

Readable Message

BE SURE TO DRINK YOUR OVALTINE.

Message #3

85833 56315 76364 90522 20999
83620 56930 50951 67152 05400

Message #3 (Solution)

85833 56315 76364 90522 20999

83620 56930 50951 67152 05400

8 5 8 3 3	5 6 3 1 5	7 6 3 6 4	9 0 5 2 2	2 0 9 9 9
8 5 8 3 3	2 7 3 8 5	1 2 5 3 6	4 8 8 7 7	4 7 6 3 0
K E Y I D	7 3 6 9 0	8 8 8 9 0	3 8 3 9 9	6 7 5 2 9
	F T FIG	8 FIG	I S SPC	T H E SPC

8 3 6 2 0	5 6 9 3 0	5 0 9 5 1	6 7 1 5 2	0 5 4 0 0
1 4 4 0 8	8 0 0 6 7	0 1 8 4 9	0 0 6 2 7	5 2 8 2 0
9 7 0 2 8	3 6 9 9 7	5 1 7 9 0	6 7 7 7 9	5 7 2 2 0
B E S	T SPC H	A M 0	RADIO M	O D E 0

Decoded Characters from Conversion Chart

FT FIG 8 FIG IS SPC THE SPC BEST SPC HAM RADIO MODE 0

Readable Message

FT8 IS THE BEST HAM RADIO MODE

Message #4

85833 66994 06745 69265 45379
85480 75533 85539 78371 71012
86030 24612

```
85833 66994 06745 69265 45379
85480 75533 85539 78371 71012
86030 24612
```

8 5 8 3 3	6 6 9 9 4	0 6 7 4 5	6 9 2 6 5	4 5 3 7 9
8 5 8 3 3	2 7 3 8 5	1 2 5 3 6	4 8 8 7 7	4 7 6 3 0
K E Y I D	8 3 2 7 9	1 8 2 7 1	0 7 0 3 2	8 2 9 0 9
	S E M	A R C	REPEAT E	R FIG 9

8 5 4 8 0	7 5 5 3 3	8 5 5 3 9	7 8 3 7 1	7 1 0 1 2
1 4 4 0 8	8 0 0 6 7	0 1 8 4 9	0 0 6 2 7	5 2 8 2 0
9 9 8 8 8	5 5 5 9 0	8 6 3 7 8	7 8 9 9 8 2 3 8 3 2	
8	5 FIG	W I L	L SPC R I S E	

8 6 0 3 0	2 4 6 1 2			
1 3 1 4 4	9 9 8 8 9			
9 9 1 7 4	1 3 4 9 1			
SPC A G	A I N .			

Decoded Characters from Conversion Chart

SEMARC 0 REPEAT ER FIG 985 FIG WILL RISE AGAIN.

Readable Message

SEMARC REPEATER 985 WILL RISE AGAIN.

Message #5

```
85833 52941 87633 59516 53703
85773 83894 61158 57789 25175
36933 83446 51110 21631 91871
07590 54970 33572 19976 67534
96180 19033 56209
```

Message #5 (Solution)

```
85833 52941 87633 59516 53703
85773 83894 61158 57789 25175
36933 83446 51110 21631 91871
07590 54970 33572 19976 67534
96180 19033 56209
```


Decoded Characters

MEET SPC AT SPC FS FIG 3 SPC ACTIVATE SPC HF 0 RADIO ON FIG 777 222 555 000 FIG . LISTEN SPC FOR 0 INSTRUCITONS AT SPC FIG 222 111 333 000 SPC UTC.

Readable Message

MEET AT FS 3

ACTIVATE HF RADIO ON 7250.

LISTEN FOR INSTRUCTIONS AT 2130 UTC.

KPH Message

```
14408 22398 89277 37674 58289
07722 15378 84975 30552 61128
69986 02108 68467 10079 92331
32982 54092 37446 22905 15340
17129 81152 39418 67073 25414
81456 43361
```

KPH Message (Solution)

```
14408 22398 89277 37674 58289
07722 15378 84975 30552 61128
69986 02108 68467 10079 92331
32982 54092 37446 22905 15340
17129 81152 39418 67073 25414
81456 43361
```

Readable Message

CURRENT OP COMPROMISED. ABORT.

TRAVEL IMMEDIATELY TO ISTANBUL VIA SWISS PASSORT.

CONTACT AGENT MAX.

DANGER, INSIST ON MOSCOW RULES.
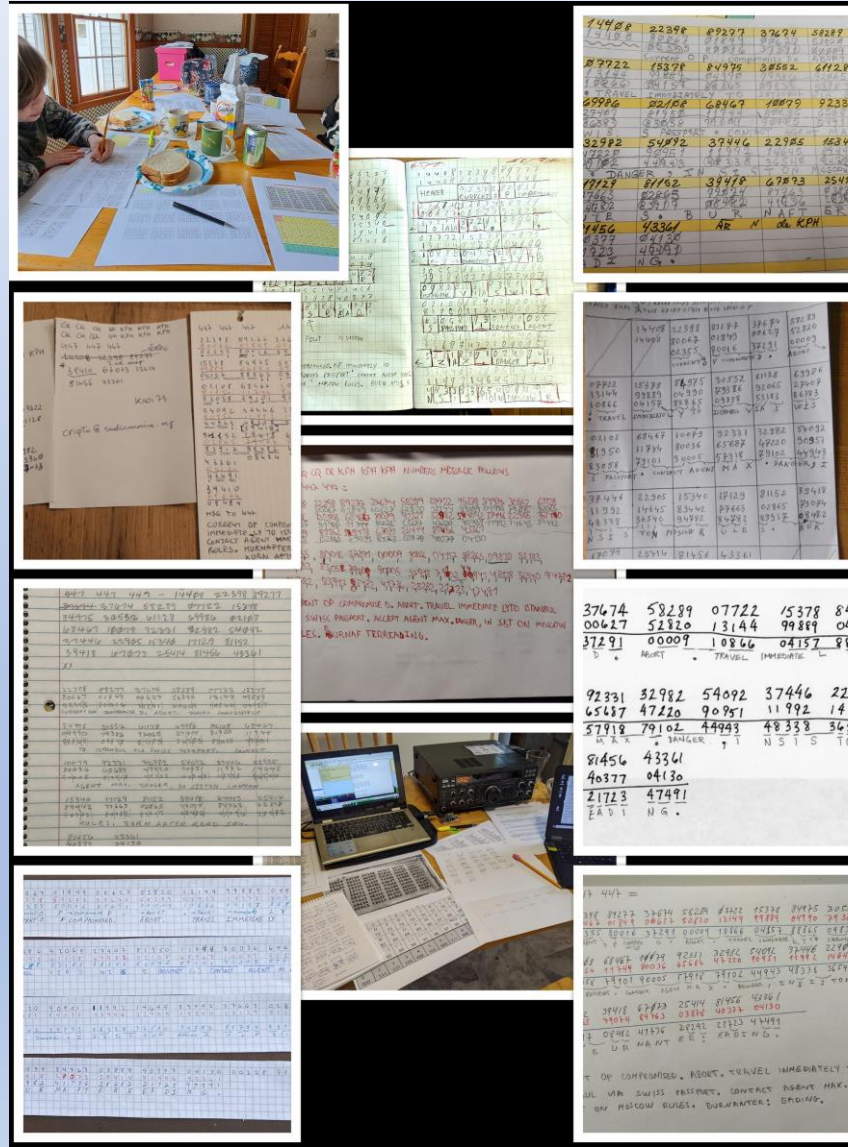
BURN AFTER READING.

Conclusion

- The KPH MRHS exercise afforded a fine introduction into the past and current employment of 5-digit numbered messages that were used in different ways and purposes over the decades.
- Cryptography has a very long history, always balancing:
  - Decrypting/encrypting difficulty
  - Decrypting/encrypting materials availability
  - Interception and decoding risk
  - Other considerations
- Some well-known encryption examples:
  - **ROT-13:** mono-alphabetical substitution cipher which has the property of being reversible and very simple. Each letter is shifted by 13 positions in the English alphabet.
  - **Ottendorf Cipher:** One symbol means a letter or word, the other is the page you can find it on in a book, newspaper or magazine. The movie National Treasure used Ben Franklin's Dogood Letters.
  - **Playfair Cipher:** encrypts using a digraph, or a pair of two letters, instead of a single letter.
  - **ENIGMA Machine**
  - Many, many others

KPH Event After Action Report

- MRHS received 161 entries and sent out 156 "Certificates of Cryptographic Excellence".

- Entries came in from US, Japan, Canada, Brazil, Argentina, Puerto Rico, Spain, France, Italy, Germany, Finland, Netherlands, England, Australia, New Zealand, Czech Republic and Poland. About 1/3 of the participants had participated in previous KPH crypto challenges.

- Decoding the Numbers Message involved 130 modulo-10 additions (one for each digit in the message), converting the resulting digits back to letters using the supplied conversion chart and the use of a codebook to look up useful words and phrases.

- The first decode was received only 10 minutes after the broadcast finished, with the rest coming in within the 72-hour time limit.

KPH Event After Action Report

Bibliography

- Maritime Radio Historical Society (MRHS)
  - https://www.radiomarine.org/mrhs-events (After Action Report)
  - https://www.radiomarine.org/events-2 (Mission Critical documents)
- Crypto Museum
  - https://cryptomuseum.com/crypto/otp/index.htm (OTP description/discussion)
  - https://cryptomuseum.com/crypto/enigma/index.htm (Enigma machine)