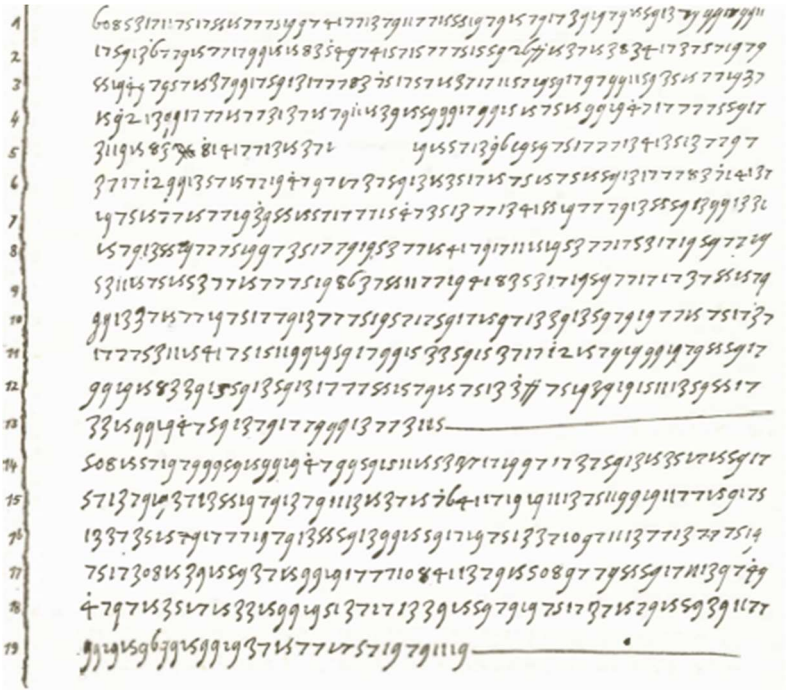
Cryptography Compressed

By Melchior zum graun Wolf (Kevin Baun)

Prior to his death, in July of 1572, Sigismund II managed to broker an uneasy peace between the Catholics and Protestants. He also oversaw the Union of Lublin in 1569 which united Poland and Lithuania. After his death this void of leadership lead to considerable intrigue between the Vatican and various claimants. Catherine de Medici waged a campaign and eventually succeeded in gaining the approval of the Vatican for her son, though they initially supported other parties, and so Henry of Valois was elected as King of the Polish-Lithuanian Commonwealth in 1573. Henry, however, being displeased with the court politics of his mother and former tutor, Jean de Monluc (Bishop of Valence), signed the Henrician Articles which gave Poland's nobility the right to elect its own monarch and, upon the death of his brother Charles IX, he returned to France to be crowned Henry III (Leighton, 1969).

The correspondence documents of Antonio Maria Gratini, specifically a letter from the period between Henry's election and his arrival in state, secretary to Cardinal Commendone, papal nuncio to Poland, discuss a wide variety of topics and outline a network of sources ranging from Paris to Constantinople to Moscow. These writings are decidedly political in nature but touch on nothing that would not have been public knowledge. One entry of particular interest is a reference to *'un poco di cifra'*, which is a separate page included with Antonio's letter and consisting of a long series of cipher numbers and symbols. This numeric cipher aligns with numerals in the plaintext letter but the key is not included. This cipher, seemingly a common numeric substitution cipher, would go on to keep its secrets for nearly 400 years.



un poco di cifra, (Gratini, 1573)

Attempts to decipher the code revealed that the numeric sequence is composed of digraphs, a few trigraphs, and even fewer monographs. The last of which includes an inverted 4 with a dot over it, unique among the substitutions. Analysis began by looking at common cryptographic systems of the time. The most common of which was the family of nomenclature ciphers. Nomenclature ciphers use a mix of monoalphabetic and code list substitutions for common words or phrases. These ciphers are known to be in use in the Italian states and by Papal Cipher Secretaries (such as the Argenti) since before the 15th century and significantly increased in complexity over time and eventually taking on complicated multivariate systems. These cipher systems remained in use well into the 16th century.

Common features of these ciphers include: use of nulls, lack of punctuation, no doubling of consonants. Using this as well as the knowledge that *'[during this period] only [such] simple ciphers were used for papal communications in Poland, Sweden, and Germany'* (Meister,1906) the cipher may be more thoroughly analyzed. Working under the premise of a simple (multivariate monoalphabetic non-affine) cipher the enciphered text may be evaluated using crypto analytic methods of the period, namely frequency analysis and relative comparison with similar ciphers of the period.

Papal ciphers of the 1550-70s, in use

The Gratini cipher mingles several important techniques of substitution ciphers. Substitutions are performed with multivariate mappings, the letter A can be represented by 5 or 15, for example, as well as whole ‘term’ substitutions. This technique of replacing words, concepts, or common phrases with a single entity is known as a nomenclature cipher and was extraordinarily popular throughout the period. We also see the introduction of nulls to thwart attempts at cryptanalysis as well as the removal of repeating consonants. All these factors helped this code to keep its secrets for hundreds of years.

Fortunately, a similar nomenclator furnished to Cardinal Commendone when he was nuncio in Poland in 1563-1565 was discovered and cracked. The construction of that cipher is very similar to that found in the papers of his secretary, Gratini. Similarities include the numeric system for polyalphabetic substitution as well as a detailed nomenclature. Indeed, the direct alphabetic substitution appears identical so it is likely that these ciphers have a common origin.

[1563-1565] Cifra con mons. Commendone nuntio in Polonia.

null ♭																		
a	b	c	d	e	f	g	i	l	m	n	o	p	r	s	t	u	z	et con (and with)
5	35	55	75	**3**	**33**	**53**	**7**	37	57	77	**9**	39	59	79	99	**1**	31	41
15	45	65	85	**13**	**43**	**63**	17	47	67	87	19	49	69	89	73	11		
25				**23**			27				29					21		

Important things to notice are that each value ends with an odd digit: 1,3,5,7,9. Most even values are used for nomenclatures, though there are exceptions. For example, 10 maps to ‘Cardinal Varmiese’ and 20 maps to ‘Regina’. Vowels are assigned 3 substitution values to obfuscate their frequency and are the delimiters for incrementing the least significant digit while the most significant digits are incremented in a columnar fashion. Additionally, some of the 3 character mappings also apply to longer substitutions (Gaines, 1956).. 609ϟ maps to ‘Duca di Baviera’, for example. There are more than 100 known nomenclature values for this cipher.

10 99 19 ϟ 25 69 7 21 ϟ 3 27 87 609ϟ
Cardinal Varmiese to arrive in Duchy of Baviera.

Once Gratini’s cipher was identified to be using a variant of the ‘Commendone’ the bulk of the message could be decrypted and, most, nomenclature entities identified through historic context (Meister, 1906). Again, keeping in mind that that the actual decipherment of the Antonmlri cipher didn’t occur until the 1950s (Leighton, 1969; Khan, 1996).

A novel variant of 16th Century Papal Ciphers used in Germany and Poland

Using the systems outlined above, providing our own nomenclature, and extend the alphabet, we can create a unique cipher that is based entirely on period sources and structure. I will begin by assigning the possible value sets to the alphabet in use. This will be extended with a series of null values which will be randomly assigned within the cipher text. I have chosen to use common mathematical symbols for my null values as a means to thwart analysis. Finally, a nomenclature of common words and phrases is defined. The process of encryption is as follows: nomenclature, removal of repeating consonants, character substitution, random assignment of nulls. The resulting cipher key is shown below.

Substitution Cipher Key

null +, -, =

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
5	35	55	75	**3**	33	53	73	**7**	37	57	77	97	117	**9**	39	59	79	99	119	**1**	31	51	71	91	111
15	45	65	85	13	43	63	83	17	47	67	87	107	127	19	49	69	89	109	129	11	41	61	81	101	121
25				23				27						29						21					

Example Nomenclature

Atlantia	20	message	70
cipher	30	and	80
secret	40	It is	90
King	50	war	100
Queen	60	science	10

References:

Bauer, F.L. (2002). Decrypted Secrets: Methods and Maxims of Cryptology. Springer.

Gaines, H. F. (1956). Cryptanalysis; a study of ciphers and their solution. New York: Dover Publications.

Holden, J. (2017). The Mathematics of Secrets: Princeton University Press.

Kahn, D. (1996). The codebreakers: The story of secret writing. New York: Scribner.

Leighton, A. (1969). A Papal Cipher and the Polish Election of 1573. *Jahrbücher Für Geschichte Osteuropas, 17*(1), neue folge, 13-28. Retrieved April 20, 2020, from www.jstor.org/stable/41044190

Meister, A. (1906). Die Geheimschrift im Dienste der papstlichen Kurie.

119 73 7 109 7 109 15 48 66 119 19 119 73 23 49 23 19 49 87 23 19 43 22 7 23 117 55 19 1 79 15 63 23 101 19 1 119 19 55 19 117 109 7 75 23 79 119 73 23 31 15 87 1 23 19 43 26 109 55 19 75 23 109 72 119 73 23 109 23 55 1 79 7 119 101 19 43 7 117 43 19 79 107 15 119 7 19 117 119 73 7 109 117 19 45 87 23 109 55 7 23 117 55 23 51 15 109 23 107 49 87 19 101 23 75 45 101 50 109 72 64 109 43 19 79 73 1 117 75 79 23 75 109 19 43 101 23 15 79 109 51 7 119 73 7 117 19 1 79 119 7 107 23 49 23 79 7 19 75 19 43 109 119 1 75 101 87 7 31 23 109 72 43 19 79 119 1 117 23 109 51 23 79 23 107 15 75 23 72 87 19 109 119 19 31 23 79 119 73 23 109 119 79 23 117 63 119 73 19 43 15 48 119 73 23 109 119 1 75 101 19 43 26 109 15 75 75 109 119 19 19 1 79 67 117 19 51 87 23 75 63 23 19 43 119 73 23 109 55 7 23 117 55 23 109 72 23 117 79 7 55 73 23 109 19 1 79 1 117 75 23 79 109 119 72 7 117 63 19 43 119 73 23 23 31 23 117 119 109 119 73 15 119 119 73 23 101 7 117 43 87 1 23 117 55 23 75

79 23 109 49 23 55 119 43 1 87 87 101 107 23 87 55 73 7 19 79 121 1 107 63 79 15 1 23 117 51 19 87 43

This is a secret message to the people of Atlantia. I encourage you to consider the value of ciphers, codes, and the security of information. This noble science was employed by kings and queens for hundreds of years within our time-period of study. Lives and fortunes were made and lost over the strength of a secret. The study of ciphers adds to our knowledge of the sciences and enriches our understanding of the events that they influenced

- Respectfully Melchior zum grauen Wolf

Simple programmatic implementation, encoding

```
<script>
// This small script performs the multi-variant & whole word
// replacement for a given string.
var strOrg = "String to encode";
var str = strOrg;
function getRando(inputArray){
       var randVal = inputArray[Math.floor(Math.random() * inputArray.length)];
       return randVal + " ";
}
str = str.toLowerCase();

str = str.replace(/atlantia/g,"20 ");
str = str.replace(/cipher/g,"30 ");
// …
str = str.replace(/war/g,"100 ");
str = str.replace(/science/g,"10 ");

str = str.replace(/a/g,getRando(["5","15","25"]));
str = str.replace(/b/g,getRando(["35","45"]));
// …
str = str.replace(/y/g,getRando(["91","101"]));
str = str.replace(/z/g,getRando(["111","121"]));

document.write(strOrg);
document.write("<br/><hr/><br/>");
document.write(str);
</script>
```