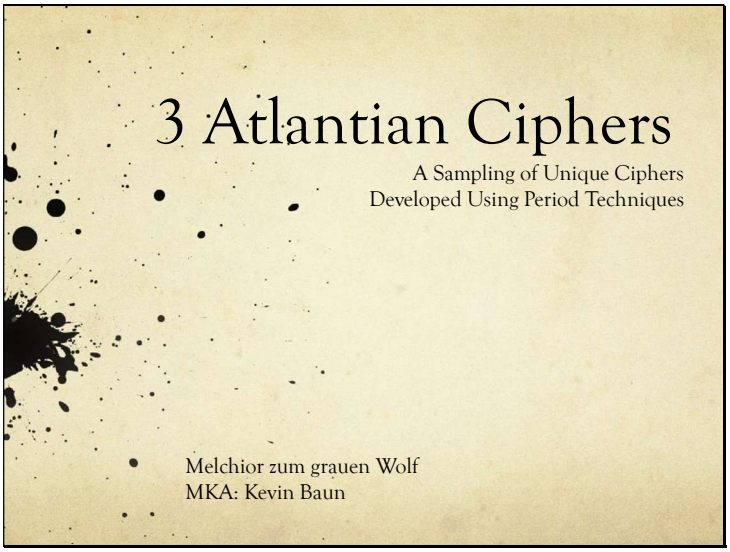
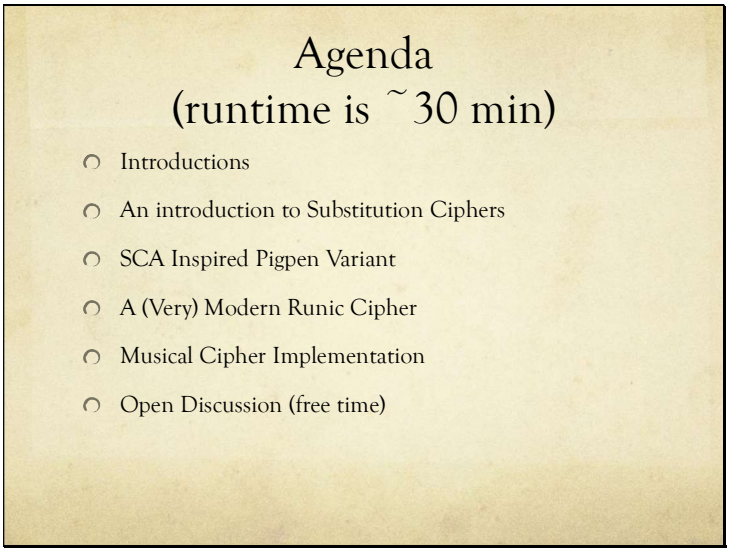
Slide 1



In this class, I introduce three ciphers of my design based on period examples. Each cipher is evaluated in three steps. First, I review the source material that the cipher is drawn from. Next, I present the cipher technique and example using the period reference. Finally, I offer an example of the implemented cipher variant. Once each cipher has been discussed I will open the floor to discussion on how period cryptography might be used in the modern middle ages.

-Melchior zum grauen Wolf

Slide 2

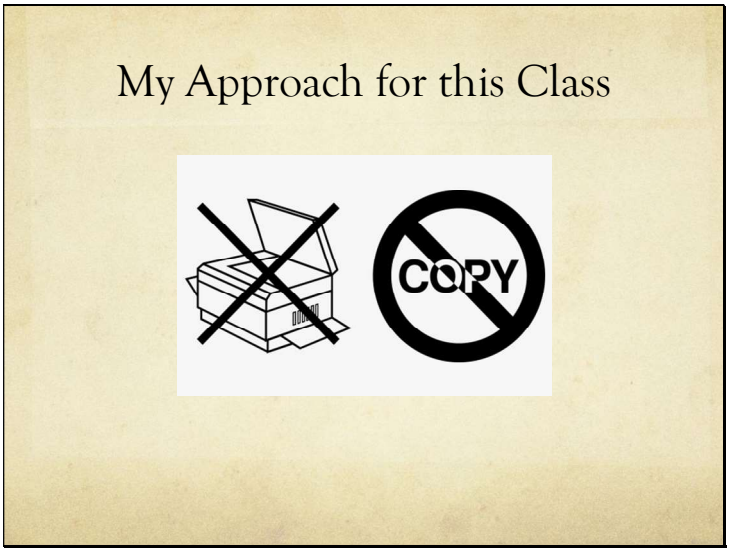


Hello and welcome

Slide 3

https://www.qr-code-generator.com/
This is the first time that I'm teaching this class so I'd like to learn a little about what you're interested in. What brought you to this class?
go around the room

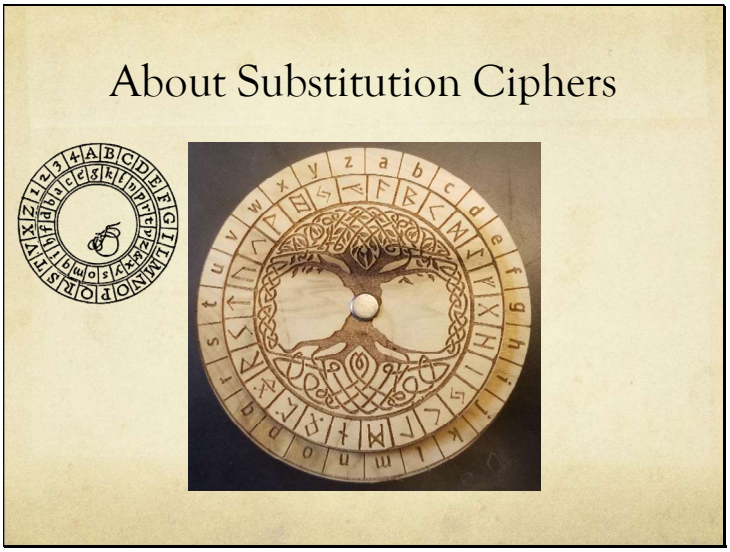
Slide 4



I have no interest in being a medieval photocopier. Do not expect this class to show faithful and accurate reproductions of extent examples. I have no interest in that beyond learning how the work was done so that I can learn the techniques. I leave that kind of reproduction work to those that do that thing. I will be showing some period examples for context and for contrast, but the core of the class is on creating something new using period techniques.

So… documentation is provided but only so much as to support the foundation needed to make something new. If you're interested in more research/documentation on period materials then please attend one of my research classes on cryptography. There are several and I'm happy to nerd out with you 1 on 1.

Slide 5



The ciphers we will be discussing today all broadly fall into the class of substitution ciphers. This is exactly what it sounds like. Letters, groups of letters, whole words, and even concepts are exchanged for the cipher text. There are many variation on this approach. Some of those are relatively simple, consider the Caesar Cipher – also known as a rotational or (ROT) cipher. This is a simple approach where the cipher text for the plaintext alphabet shifts by a predetermined number. A becomes D, B becomes E, and so on. Other systems are highly complex. Francis Bacon's bi-literal cipher employs a binary encoding mechanism, for example. We will briefly discuss some of these ciphers in our discussion today but, again, the focus of this presentation is on novel implementations and not on reproduction.

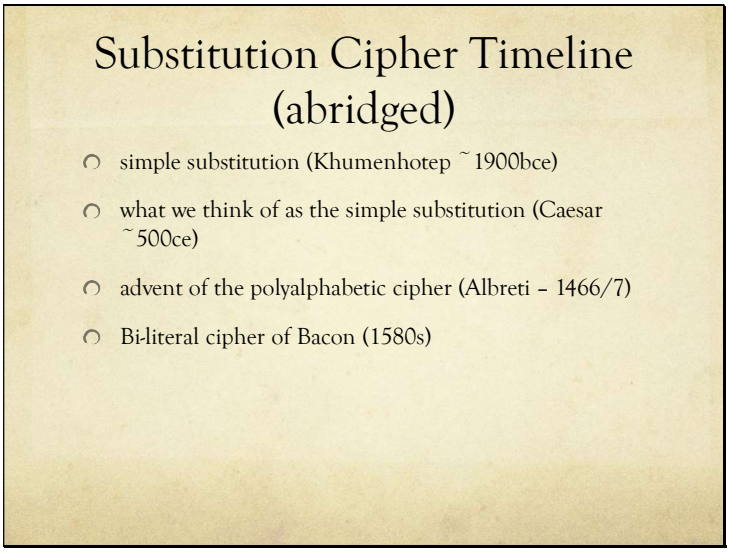
The device you see here is one of my own design and construction based on the Albreti 'formula' as described in '*De componendis cifris*' (1467), shown on the left. In this design the outer ring (stabilis) represents the plaintext alphabet while the inner ring (mobilis) could be oriented according to a predetermined index. In that simple use case a degree of complexity is introduced (notice that the mobilis does not follow the natural letter order). Of particular interest for this approach is that by introducing a key word the formula may achieve a polyalphabetic cipher text. That is, each letter of the plaintext may be represented by multiple cipher text characters.

In my implementation here you will notice that the cipher text is represented using runes. The futhark being an alphabet of only 24 characters also allowed for the opportunity to introduce new glyphs to further confound any potential analysis. So, as we see here, I have taken a

completely period technique and implemented it in a new and novel way. This is the approach that I attempt to follow throughout this presentation.

The image on the left is used under the Creative Commons license and is available here: https://commons.wikimedia.org/wiki/File:Alberti_cipher_disk.svg

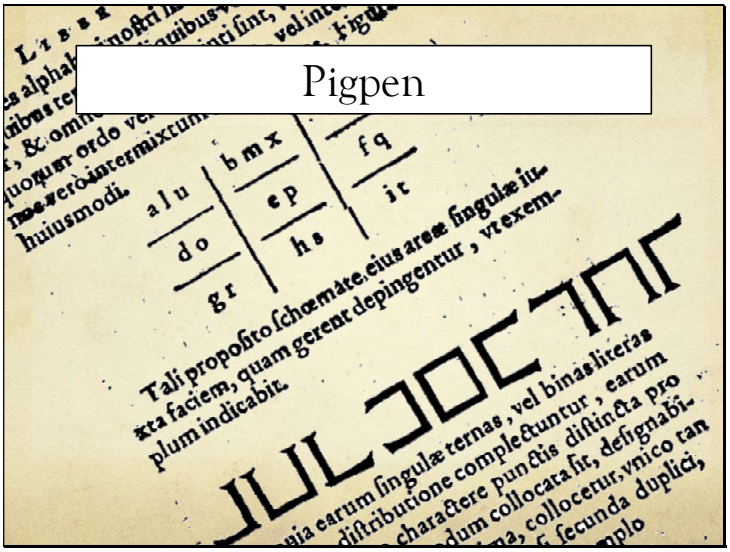
Slide 6



A final note on substitution ciphers, these ciphers have a long history throughout the western world. The prevailing theory at this time is that what we think of as a 'substitution cipher' began as a method for scribes in ancient Egypt to embellish hieroglyphics with variations in the text using embellishments such as multiple regional dialects as a method of advertising their skill and craftsmanship. I, personally, find this to be a fascinating beginning to this science because in being used in this way what we think of as 'cryptography' was actually a method of drawing attention to the meaning of a text rather than concealment.

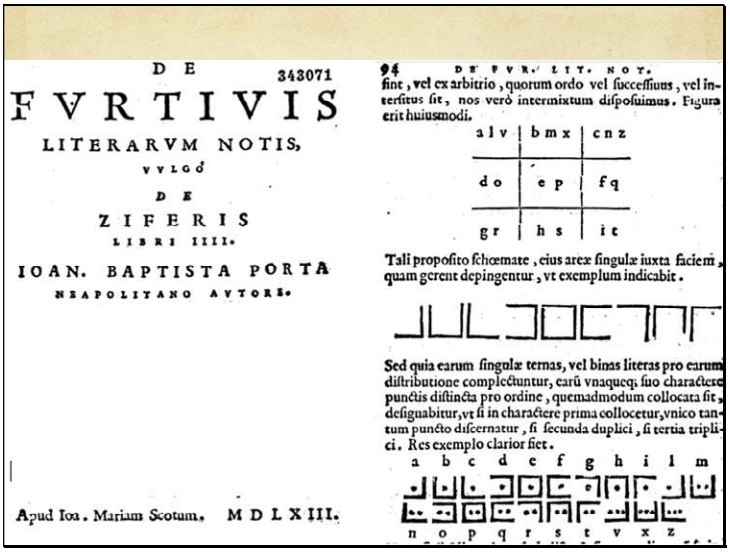
Before anyone asks the question, this would be a good place to talk about the difference between cryptographic systems and steganographic ones. Cryptographic systems are overt. There is generally little to no attempt to conceal the fact that what is on the page is a cipher of some kind. Steganographic systems, on the other hand, are covert and attempt to conceal the presence of a message at all. These systems were frequently used together throughout history but it is important to understand the distinction between the two.

Slide 7



We will begin our little journey with one of the most well known substitution ciphers. This is known as the 'Pigpen' or sometimes called the 'Freemasons' cipher due to its somewhat frequent use in the headstones of prominent Freemasons beginning around the turn of the 18th century. While the true origins of this cipher are unknown we know, and will show, that this was a cipher known in period and was referred to in that time as being of ancient roots.

Slide 8



D E 343071
FVRTIVS
LITERARVM NOTIS,
VVLGÒ
DE
ZIFERIS
LIBRI IIII.
IOAN. BAPTISTA PORTA
NEAPOLITANO AVTORE.

Apud Ioa. Mariam Scotum. M D L X III.

94 DE FVR. LIT. NOT.

sint, vel ex arbitrio, quorum ordo vel succeſſiuus, vel interſitus ſit, nos verò intermixtum diſpoſuimus. Figura erit huiusmodi.

a l v	b m x	c n z
d o	e p	f q
g r	h s	i t

Tali propoſito ſchœmate, eius areæ ſingulæ iuxta ficiem, quam gerent depingentur, vt exemplum indicabit.

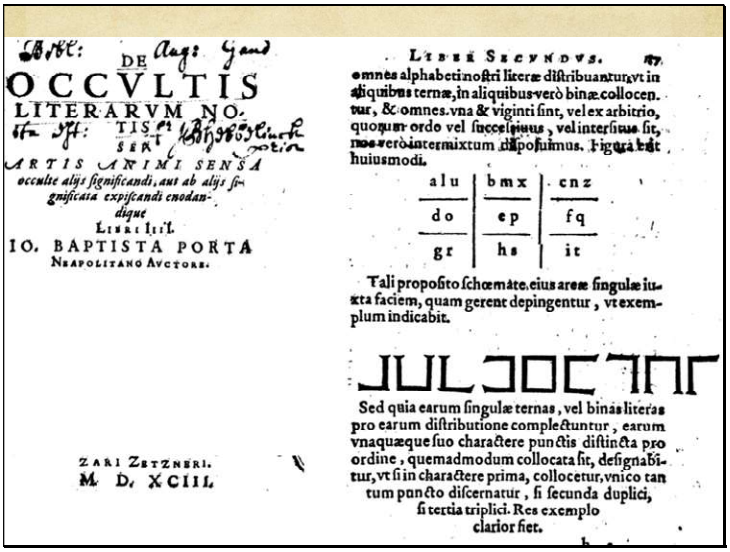
Sed quia earum ſingulæ ternas, vel binas literas pro earum diſtributione complectuntur, earũ vnaqueq; ſuo characterc punctis diſtincta pro ordine, quemadmodum collocata ſit, deſignabitur, vt ſi in characiere prima collocetur, vnico tantum puncto diſcernatur, ſi ſecunda duplici, ſi tertia triplici. Res exemplo clarior fiet.

a b c d e f g h i l m

n o p q r s t v x z

Here we have scans from the 1563 edition of Porta's 'De FURTIUS' showing the 'pigpen' structure and an example of the cipher in use. Notice the deconstruction of the alphabet at the bottom of the page and how pips are used to indicate which letter within each structure to be used.

Slide 9



DE
OCCVLTIS
LITERARVM NO-
TIS
SER
ARTIS ANIMI SENSA
occulte alijs significandi, aut ab alijs significata expiscandi enodandique
LIBRI III.
IO. BAPTISTA PORTA
NEAPOLITANO AVCTORE.

ZARI ZETZNERI.
M. D. XCIII.

LIBER SECVNDVS. 87

omnes alphabeti nostri literæ distribuantur, vt in aliquibus ternæ, in aliquibus verò binæ collocentur, & omnes vna & viginti sint, vel ex arbitrio, quorum ordo vel successiuus, vel intersitus sit, nos verò intermixtum disposuimus. Figura hæc huiusmodi.

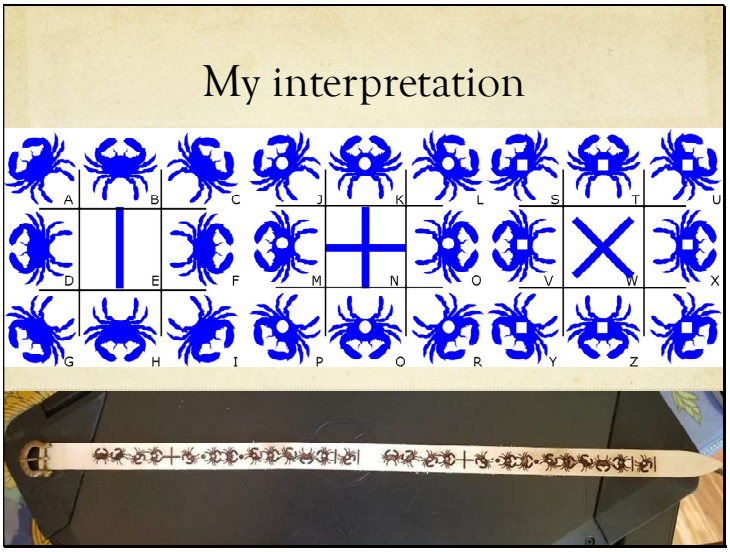
alu	bmx	cnz
do	ep	fq
gr	hs	it

Tali proposito schœmate eius areæ singulæ iuxta faciem, quam gerent depingentur, vt exemplum indicabit.

Sed quia earum singulæ ternas, vel binas literas pro earum distributione complectuntur, earum vnaquæque suo charactere punctis distincta pro ordine, quemadmodum collocata sit, designabitur, vt si in charactere prima, collocetur, vnico tantum puncto discernatur, si secunda duplici, si tertia triplici. Res exemplo clarior fiet.

Here we see Porta return to describe the cipher again in 1593's 'De Occultis', again following the same patterns.

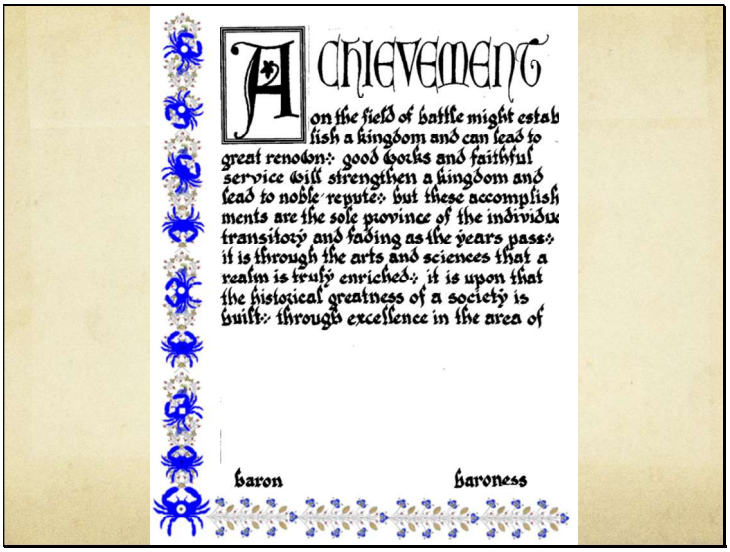
Slide 10



A Novel Simple Cipher for the Modern Middle Ages

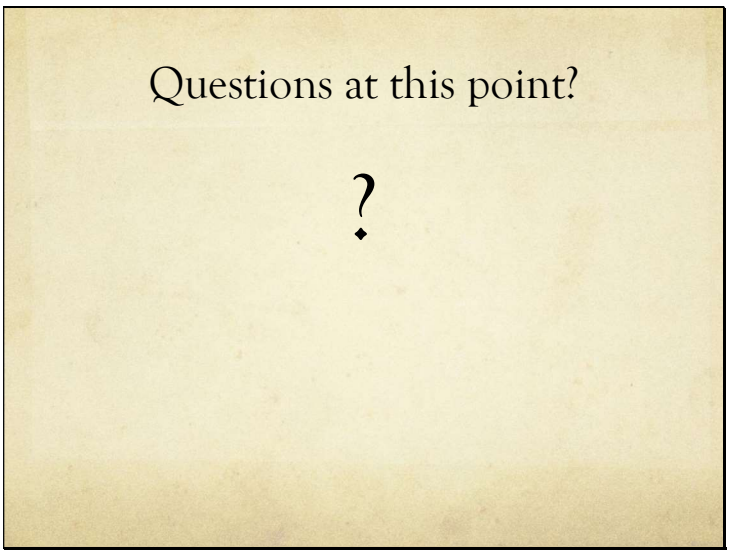
The pictographic cipher shown below is based on the 'Pigpen cipher' and uses the orientation of a common symbol, in this case the crab of Lochmere, in conjunction with 'dots' to signify which letter to use in a given position. Period examples of this type (see Porta, 1563) use the angulations provided by the 'hash' divider such that the top left quadrant would hold the letters A, J, and S. The modern 26-character western alphabet does not nicely align with the 27 available positions within the three iterations of the cipher matrix so I have elected to employ another period technique and add a character which is substituted for an entire word (Trithemius, 1461). In this case the central pictograph represents the word "Atlantia". While this has no practical impact on subverting cryptanalysis it is a fun way to fill out the space. This cipher key is provided along with an example of how such a cipher could be used within the SCA. The provided example, see be, uses the cipher designs within the border of a scroll blank or promissory note. Can you decipher this hidden message? What other ways can you think to use period cryptography in the modern middle ages?

Slide 11

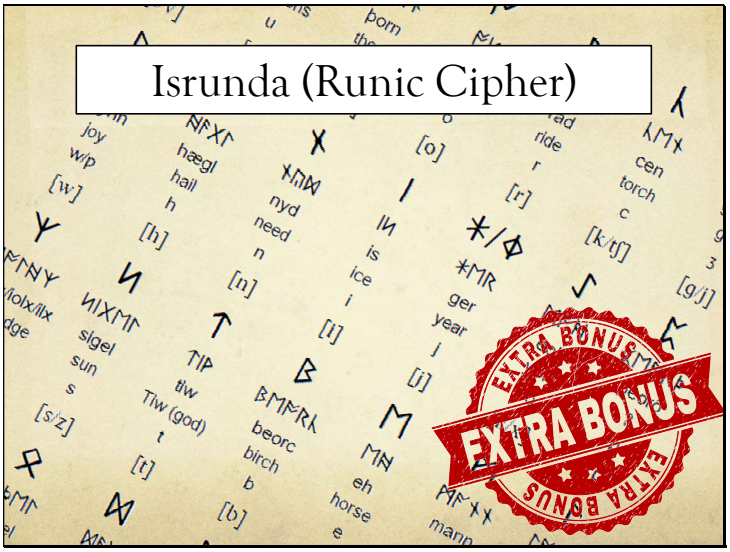


This shows another potential use of the cipher mixed in with a scroll. This example uses a slight variation to the key we saw on the last slide but I'm sure you can work it out. 'Lochmere Atlantia', here the bottom large crab with the dot represents a whole word 'Atlantia' showing how a nomenclature cipher could be worked to intermix with the pigpen system. Mixing ciphers was done throughout period and across regions so that technique is well known and has many examples.

Slide 12



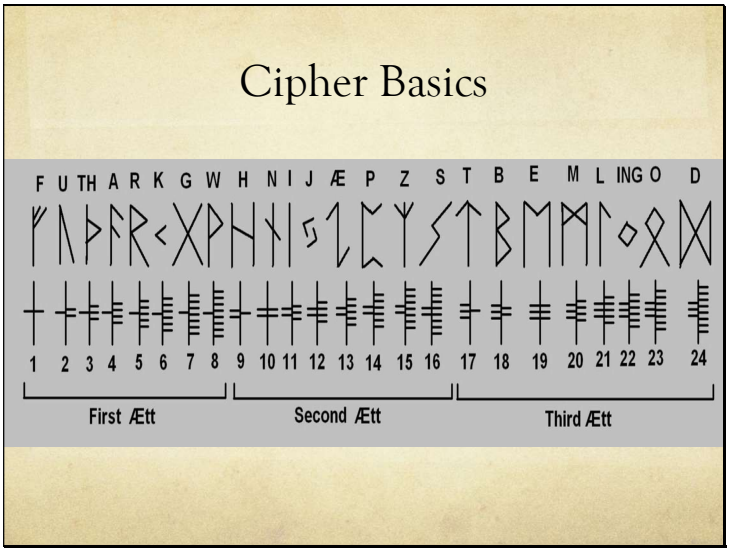
Slide 13



Now let's talk about runes and how we can abuse them for our own nefarious cryptographic needs. Runes are interesting to me because each symbol carries phonetic value, a transliteration value, and an inherent 'meaning'. The history of runes and how they can be used to conceal messages is fascinating but also out of the scope of this class. I teach a whole class on runic ciphers if you're interested in such things. Finally , you will notice the large red bonus logo there. There is a cipher of my design that can be found implemented by a fine craftsperson throughout the kingdom. If you are interested in playing that little game then this section may be of interest to you *cough*foot stomp*

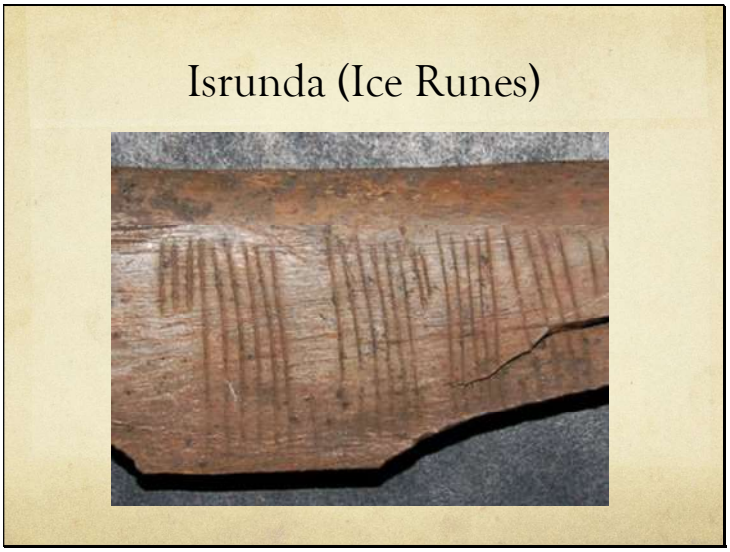
https://www.omniglot.com/writing/futhorc.htm

Slide 14



Each of the runic encoding systems relies on a common mechanism for encoding. The primary difference between them being the execution of the encoding. In this diagram we see the Elder Futhark broken into three groups of eight runes. Each group represents the initial coordinate. The position of the desired rune within the group provides the second coordinate. Please take note of the numbered straight-line characters. The U character, for example, has one bar on the left and two bars on the right. These bars identify the rune by its index of one and two. These are very simple examples of Hahalruna, which we is covered in my class on rune ciphers. The essential system is directly transferrable to the system we are using, Isruna, or Ice runes, sometimes called ‘scratch runes’.

Slide 15

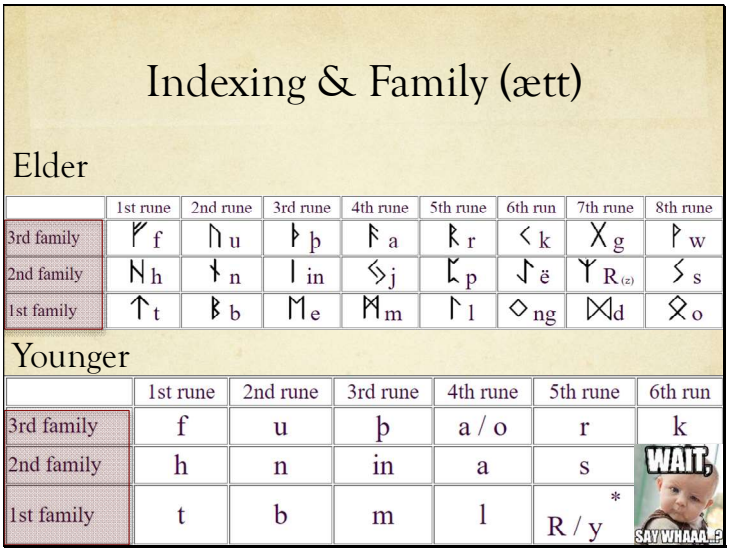


Etched in (whale) bone. (Sigtuna, Sweden)

Here we see an example of the encoding mechanism that we introduced on the previous side. Can you tell which is the aett and which represents the rune index? Remember that the aett will never be represented by more than 3 lines.

Khan, page 88
https://www.sacredequinox.com/pdfs/mithras_usa.pdf

Slide 16



Indexing & Family (ætt)

Elder

	1st rune	2nd rune	3rd rune	4th rune	5th rune	6th run	7th rune	8th rune
3rd family	f	u	þ	a	r	k	g	w
2nd family	h	n	in	j	p	ë	R (z)	s
1st family	t	b	e	m	l	ng	d	o

Younger

	1st rune	2nd rune	3rd rune	4th rune	5th rune	6th run
3rd family	f	u	þ	a / o	r	k
2nd family	h	n	in	a	s	
1st family	t	b	m	l	R / y *	

Here we see the chart broken into the family groupings with an alternate, inverse, index. Sources appear to differ on these two approaches, which is why I have included it here (more about that is on the next slide). One theory is that the order of the indexing may have flipped during the time of the Vikings, though I have yet to find definitive documentation on this matter. The next thing to notice is that the same system may be applied to the sixteen-character Younger Futhark. The ‘empty values’ are simply unused, though they could be used to introduce nulls into a cipher. Again, the same encoding rules apply. Aett then index.

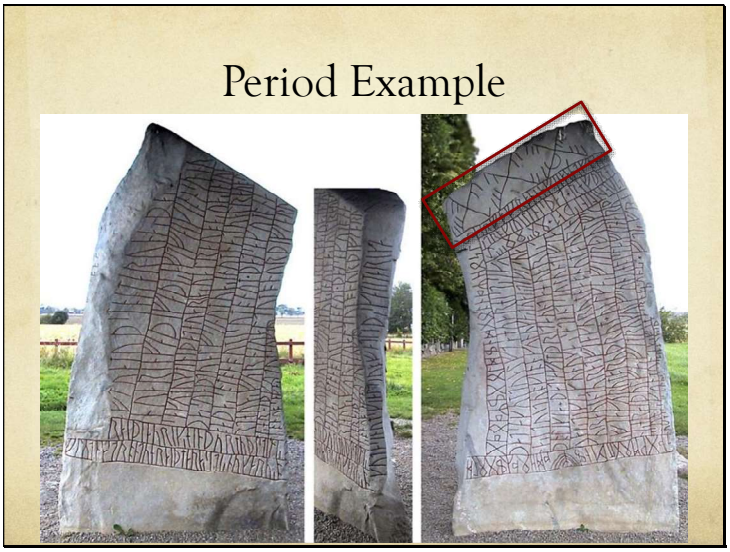
https://www.arild-hauge.com/lonnr.htm

Slide 17

Up or Down the aett?

- You may notice here that we have reordered the ætt to go from bottom up to top to bottom. Thorsson (Runelore, p89-90) suggests that either of these could be plausible and gives, as an example the stones of Krogsta (550ce) and Rotbrunna and states " [...] any method of graphically representing two numbers could be used to write cryptic messages", the reader need only be familiar with the system of dividing the ætts.
- As we're seen above the aett may be displayed in either order and in either direction. Remember that if you have a number > 3 that is your column and not the aett.

Slide 18



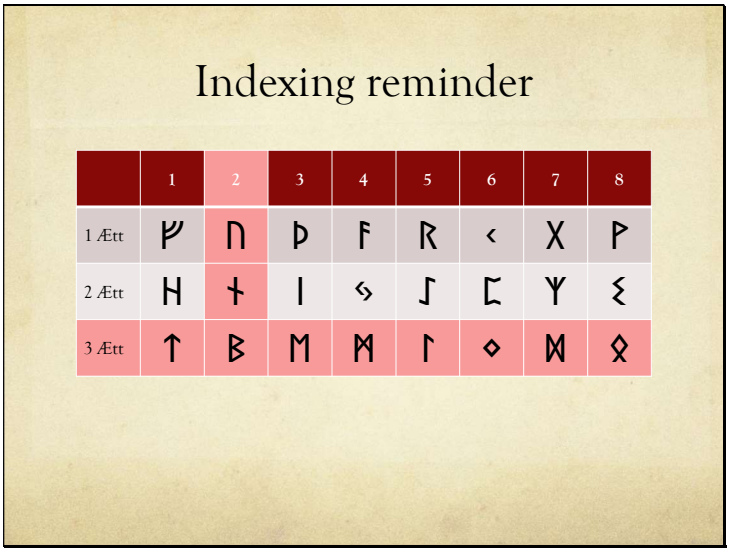
http://www.avrosys.nu/prints/arkeologi/100314.htm
Rune Stone at Rök Church, Östergötland, Sweden (early 800s)

Nearly 800 runic characters, many cipher runes.

See Rök, Östergötland, Sweden

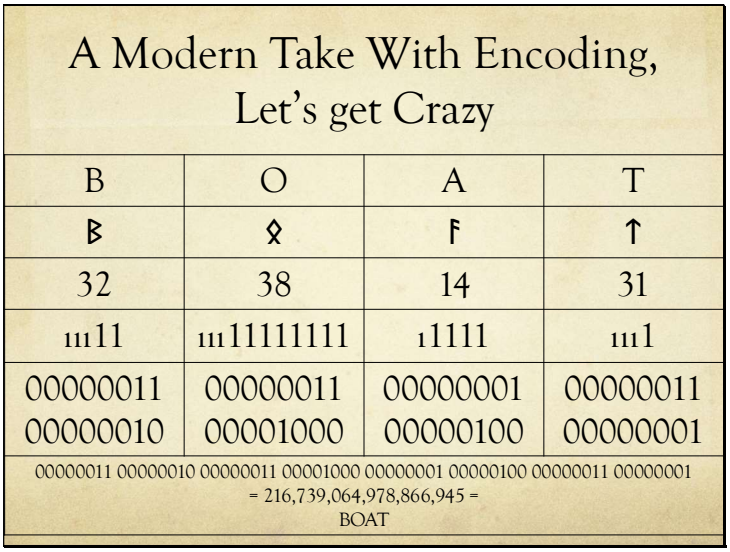
> The inscription is partially encrypted in two ways; by displacement and by using special cipher runes. The inscription is intentionally challenging to read, using kennings in the manner of Old Norse skaldic poetry, and demonstrating the carver's command of different alphabets and writing styles (including code). The obscurity may perhaps even be part of a magic ritual. (wiki - https://en.wikipedia.org/wiki/R%C3%B6k_runestone#Translation)

Slide 19



Here I've structured the aett from top down to mirror other index codes in period, such as the Greek polybus square. As you can see here the transliterated value for the letter 'B' will be represented with three marks and two marks.

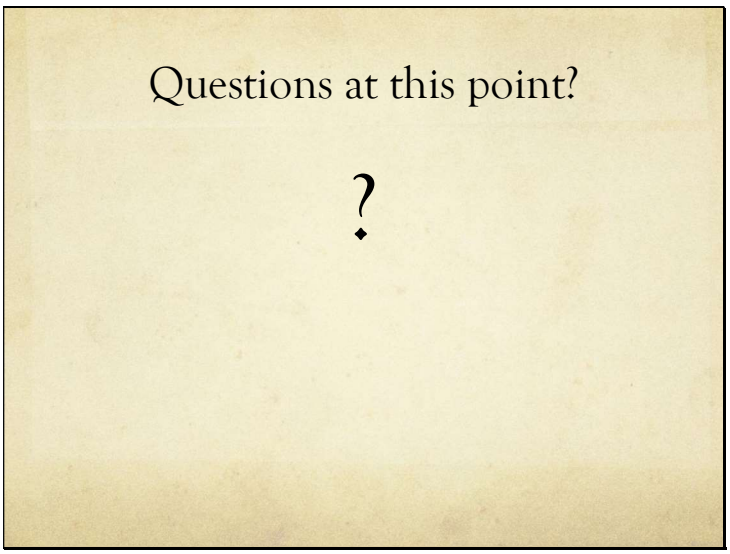
Slide 20



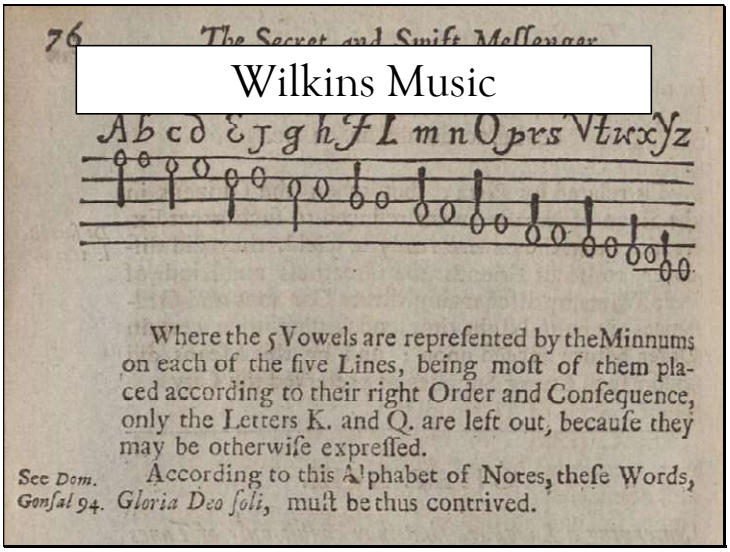
B – plain text
ᛒ - Runic value
32 – [aett][column]
iiII – Isrunda representation
Binary - First row of numbers is the binary representation of the number of the aett. Second row is binary number of the column.
Concatenated binary string = decimal representation of 216 **quadrillion …** = plaintext

As you see here we begin by transliterating the word boat into its runic value. Then we use the period technique to identify aett and index producing a decimal value. Were we using Isruna we would simply utilize the longer and shorter lines as seen in the fourth row. Finally, we convert each decimal value into a binary representation 3 = 00000011, and so on. Remembering that this technique was known to Francis Bacon in period. Each value is concatenated to create a massive binary representation which can then be converted back into decimal. The process of decryption is simply the reverse of the encryption process.

Slide 21



Slide 22

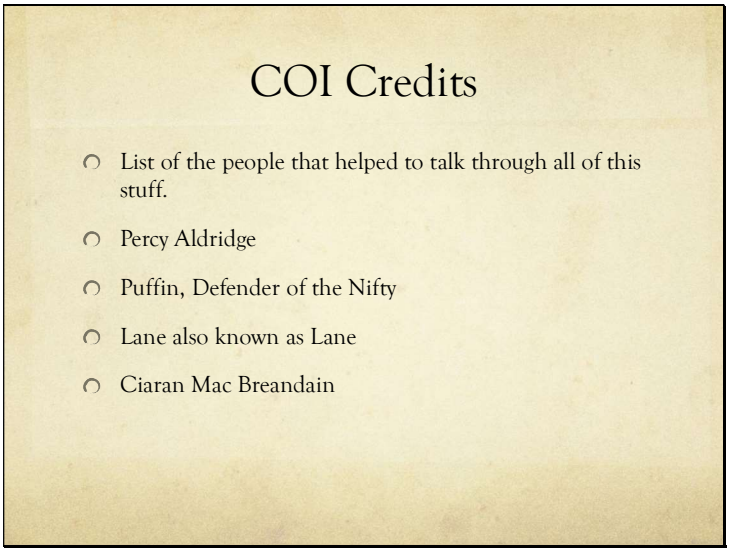


Notes

Khan notes, at the end of his chapter on 17th century cryptography that Wilkins, like his contemporary writers on the subject, is a theorist and not a practitioner of the science. These are theoretical codes and ciphers and not ones directly found as implemented correspondence.

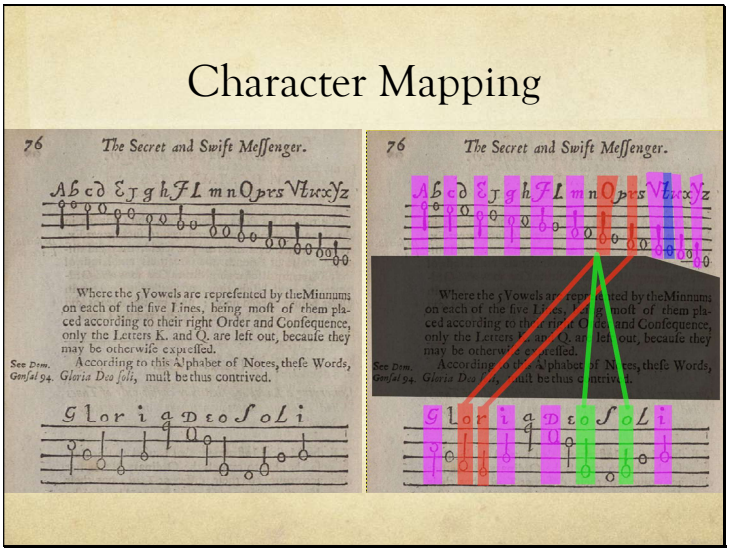
“As a genre, the cryptography manual requires scribal copying - the replication of codes, keys, and charts - as part of the learning process” – Ellison, ‘Millions of Millions of distinct orders: Multimodality in seventeenth century cryptograph manuals

Slide 23



Puffin offers to coordinate potential scribal for the score

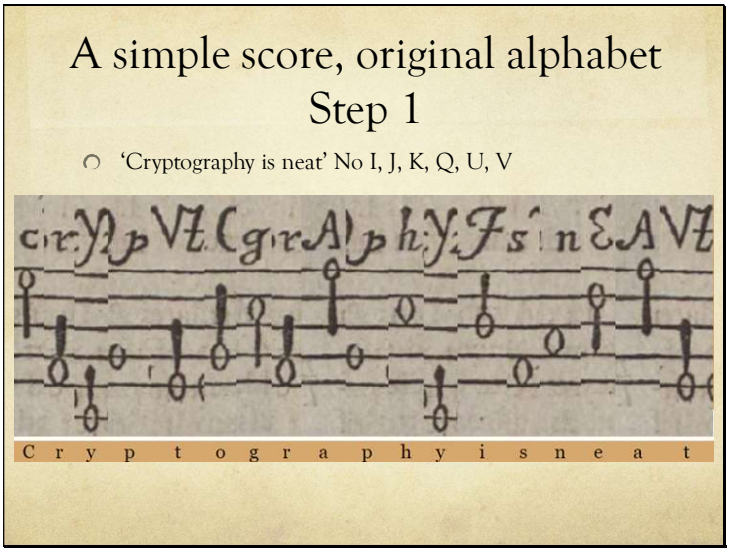
Slide 24



Here we have the original material on the left and the exemplar mapping on the right. There are two things that stand out on examination. First, it appears that the O and the R have been mixed up in the ‘Gloria’ example (shown in red) while the other O’s appear correct (shown in green.) Second, the unique VT character appears to be the letters U/V and T but reversed. The reason for this reversal is explained in the main text. Each of the 5 vowels are notes ‘on the lines’, “being **MOST** of them placed according to their right order and consequence.”. K & Q are missing as the author says that other letters can be used to represent them. I/J share a character as do U/V. This leaves us with a 22 character alphabet.

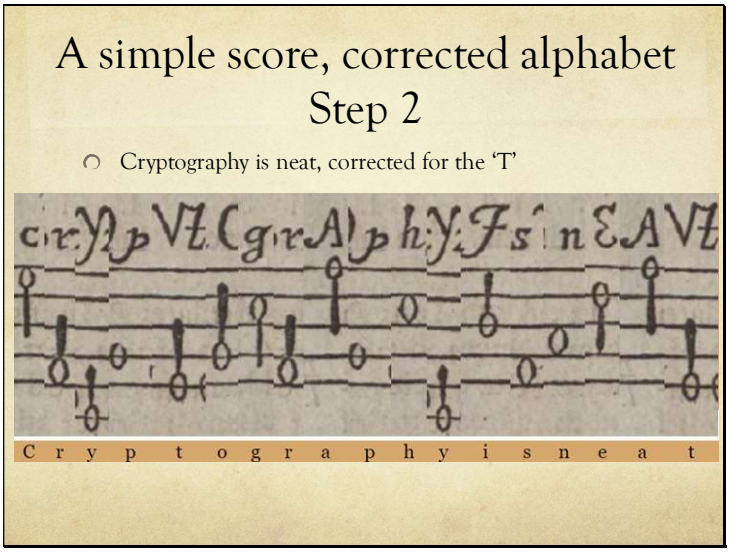
Of particular interest is that the author admits their lack of knowledge in writing music. In speaking with those more knowledgeable on the musical arts it was clearly and plainly stated that the author was, in fact, a complete idiot on these matters so we can, for our purposes, completely ignore the notion of placing vowels on the ‘lines’ or giving a care about the ‘minnums’ in our creation of a unique cipher.

Slide 25



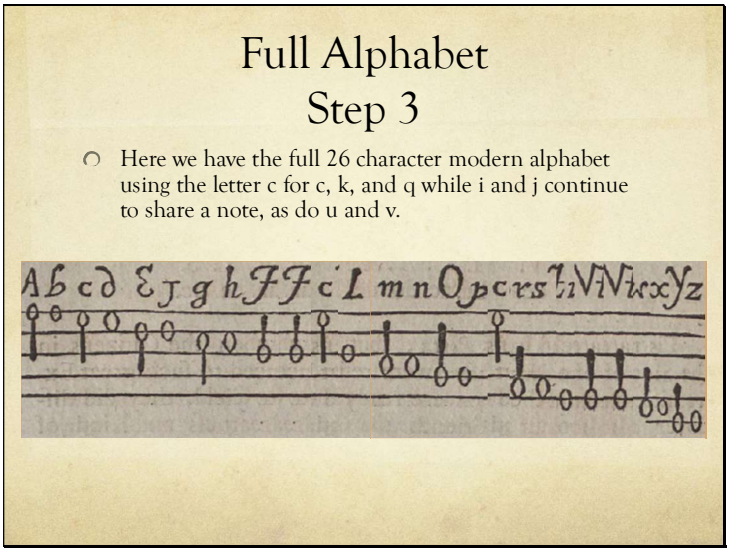
Here we have an example where I have literally sliced up the notes on the page and, using a small program that I wrote, converted text into "music" using the period approach. It sounds like to 56k modems getting hot and heavy. It does not sound good at all. Like, at all.

Slide 26



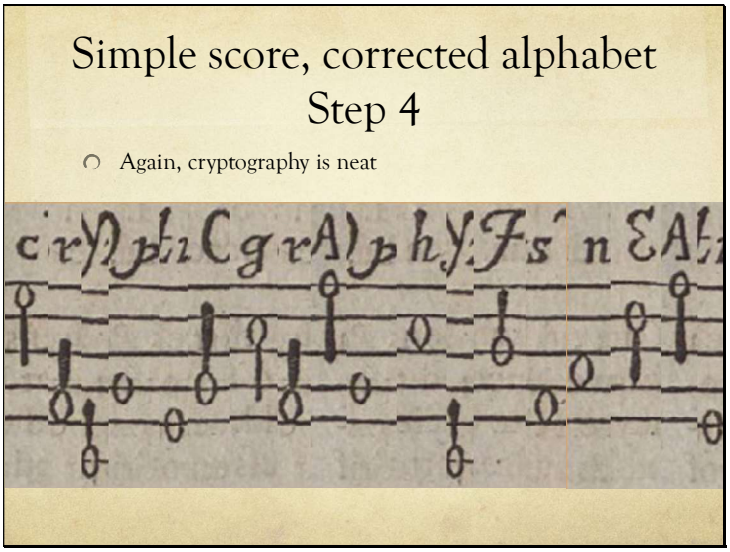
This is essentially the same as the previous slide but with a correction for the funky letter T. I show these here to outline the process that I followed.

Slide 27



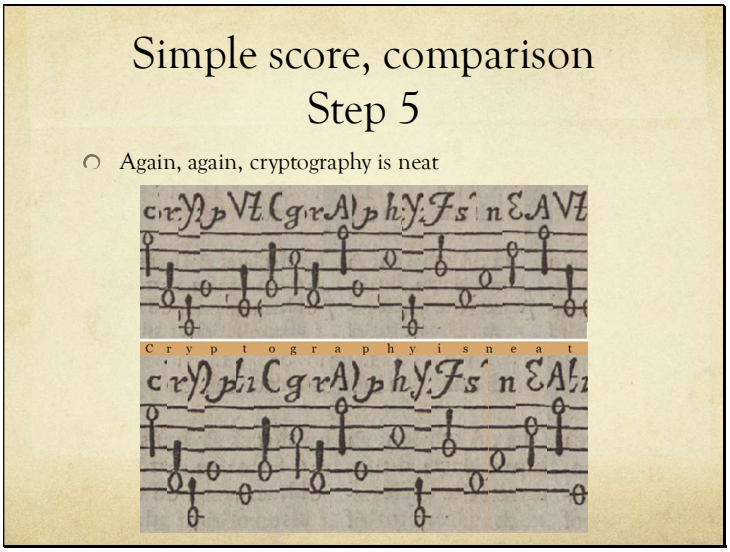
For the custom, unique cipher, I have decided to put the Q and K back in, shift the entire arrangement to the left, and reset the placement of the U/V & T so they retain their original ordering. This is a step in the right direction in that it has the full alphabet but is lacking in that there are reused characters.

Slide 28

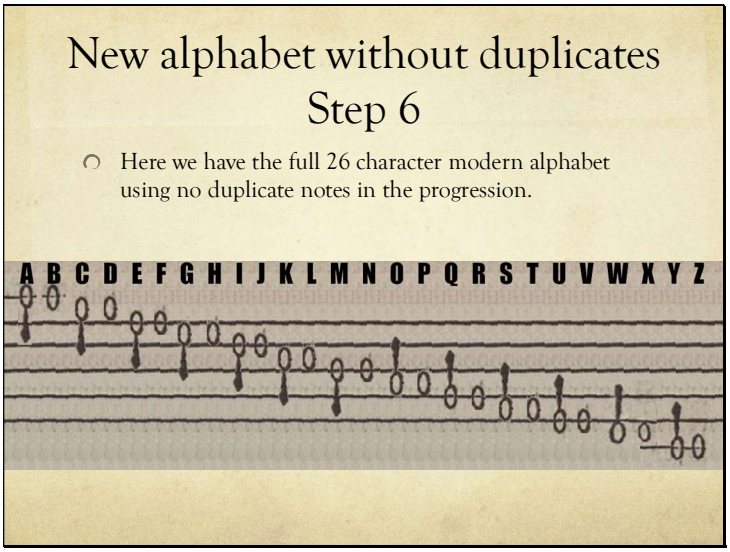


Here I once again encrypt the message but now with the ‘corrected’ alphabet. Still sounds terrible.

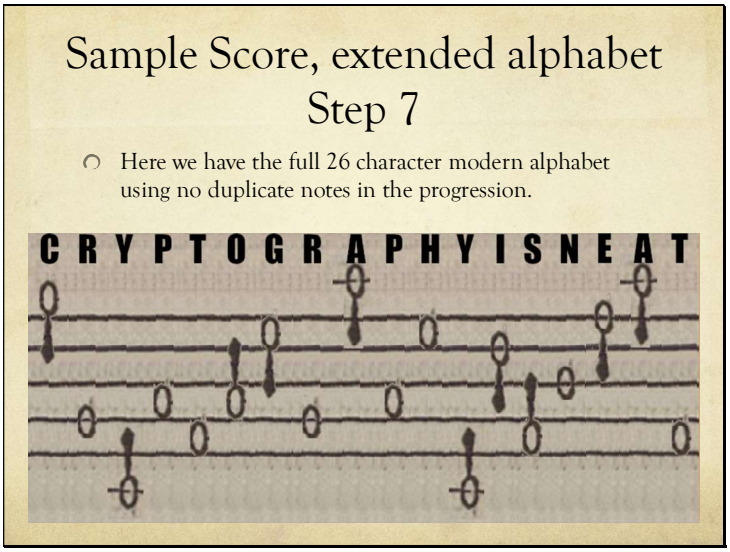
Slide 29



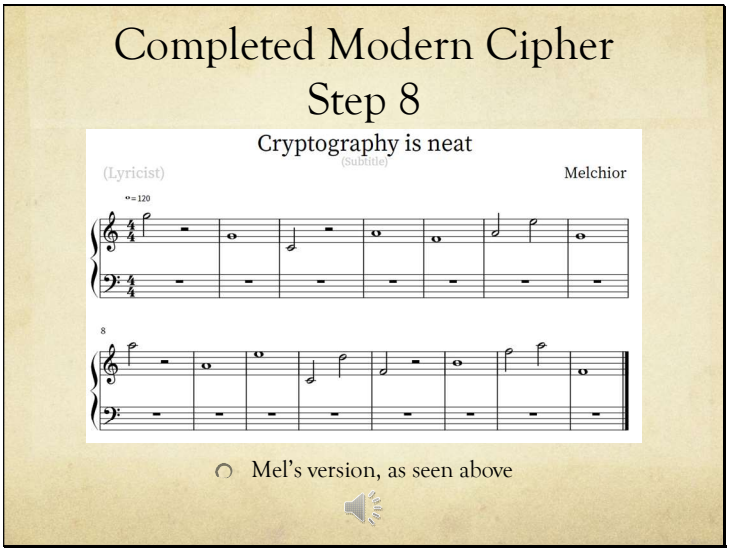
Comparing the two scores.

Slide 30

For the custom, unique cipher, I have decided to put the Q and K back in, shift the entire arrangement to the left, and reset the placement of the U/V & T so they retain their original ordering.

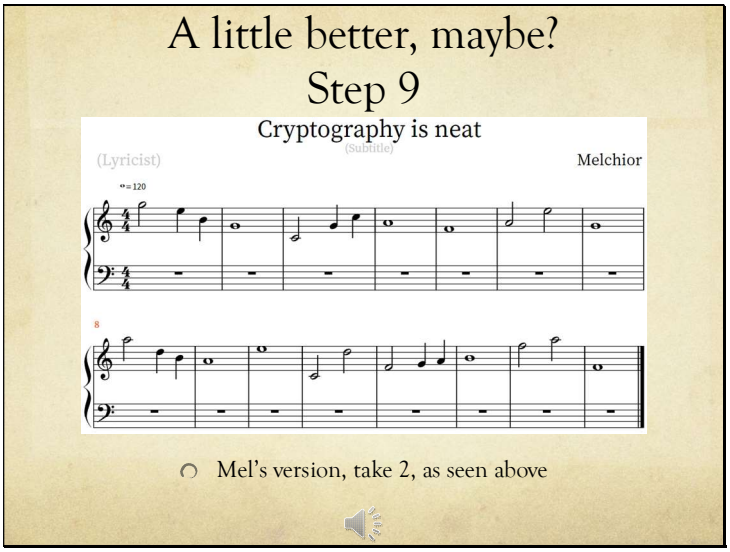
Slide 31



Here we see the test phrase corrected to use the new alphabet.

Slide 32

Cipher scored and converted to a midi using
https://www.noteflight.com/

Slide 33

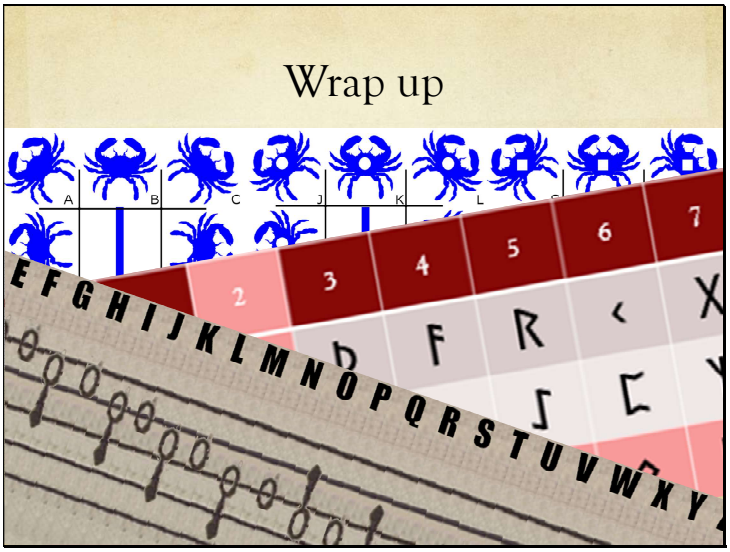
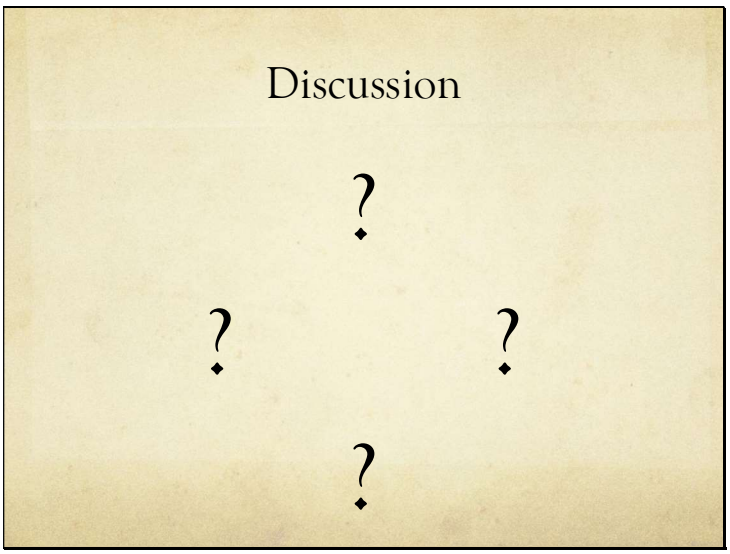

A little better, maybe?
Step 9
Cryptography is neat
(Subtitle)
(Lyricist)
Melchior
♩= 120
8
Mel's version, take 2, as seen above

Slide 34

Step 10+?

- 1/4 , 1/8, etc notes?
- If it is just whole and half notes then you can use as many 1/4 and 1/8 and trills and whatever else as you want to make it sound more like 'real' music, right?

Slide 35



Slide 36