1 Classical Cryptosystems

(Continued from previous lecture.)

1.1 Vigenere Cipher

The Vigenere cipher is our first example of a *polyalphabetic substitution*, or a substitution cipher in which the substitution scheme changes over the course of the message.

More specifically, the Vigenere cipher makes use of *modular arithmetic* and the correspondence between the letters `A` through `Z` and the numbers `0` through `25`. The **key** for a Vigenere cipher is a *finite* sequence of shifts.

A convenient and, perhaps easy-to-remember, way of constructing such a sequence is to have a secret *keyword*, and then associate each letter of that word with the corresponding number to get the sequence of shift. For example, if our secret keyword is `ASGARD`, the corresponding sequence of numbers is $(0, 18, 6, 0, 17, 3)$ because `A` corresponds to `0`, `S` corresponds to `18`, and so on.

(Example.) Suppose we want to encrypt the message `Keep Loki Away`. We begin by encoding the message through the usual way: remove all non-alphabet characters and capitalize everything.

```
KEEPLOKIAWAY
```

Then, we can associate, to each letter in the encoded message, the corresponding numbers 0 through 25.

```
 K E E  P  L  O  K I A  W A  Y
10 4 4 15 11 14 10 8 0 22 0 24
```

We can then perform addition mod 26 to each of these numbers. Specifically, we use the first element of our key sequence for the first number, the second for the second, and so on. When we finish the key, we can just repeat it from the beginning until we're done. From there, we convert those sums back to numbers using te usual correspondence. So, using the key $(0, 18, 6, 0, 17, 3)$ corresponding to the key `ASGARD` from above, we have

Encoded	K	E	E	P	L	O	K	I	A	W	A	Y
Numbers (1)	10	4	4	15	11	14	10	8	0	22	0	24
Keyword	A	S	G	A	R	D	A	S	G	A	R	D
Key Number (2)	0	18	6	0	17	3	0	18	6	0	17	3
(1) + (2) mod 26	10	22	10	15	2	17	10	0	6	22	17	1
Encrypted	K	W	K	P	C	R	K	A	G	W	R	B

From this, it follows that `KWKPCRKAGWRB` is the ciphertext.

Remarks:

- As mentioned earlier, the Vigenere cipher is polyalphabetic. Notice how the first `E` in the example above was encrypted to `W`, whilethe second `E` was encrypted to `K`.
- For decryption, the process is nearly the same. The only difference is that we *subtract* mod 26 instead of add.

(Exercise.) Using the keyword `ASGARD`,

- Encrypt the message `Protect Odin from Fenrir`.

Encoding the message gives us PROTECTODINFROMFENRIR. From there, we can label each letter:

```
 P  R  O  T E C  T  O D I  N F  R  O  M F E  N  R I  R
15 17 14 19 4 2 19 14 3 8 13 5 17 14 12 5 4 13 17 8 17
```

Noting that the key, ASGARD, has numerical correspondence $(0, 18, 6, 0, 17, 3)$, we can run through the encryption process:

```
Encoded            P  R  O  T  E  C  T  O  D  I  N
Numbers (1)        15 17 14 19 4  2  19 14 3  8  13
Keyword            A  S  G  A  R  D  A  S  G  A  R
Key Numbers (2)    0  18 6  0  17 3  0  18 6  0  17
(1) + (2) mod 26   15 9  20 19 21 5  19 6  9  8  4
Encrypted          P  J  U  T  V  F  T  G  J  I  E

Encoded            F  R  O  M  F  E  N  R  I  R
Numbers (1)        5  17 14 12 5  4  13 17 8  17
Keyword            D  A  S  G  A  R  D  A  S  G
Key Numbers (2)    3  0  18 6  0  17 3  0  18 6
(1) + (2) mod 26   8  17 6  18 5  21 16 17 0  23
Encrypted          I  R  G  S  F  V  Q  R  A  X
```

This yields the ciphertext

```
PJUTVFTGJIEIRGSFVQRAX.
```

- Decrypt the message RSMNRUOCOSTRMATG.

We begin by labeling each letter:

```
 R  S  M  N  R  U  O C  O  S  T  R  M A  T G
17 18 12 13 17 20 14 2 14 18 19 17 12 0 19 6
```

From there, we can run through the decryption process:

```
Encoded            R  S  M  N  R  U  O  C  O  S  T  R  M  A  T  G
Numbers (1)        17 18 12 13 17 20 14 2  14 18 19 17 12 0  19 6
Keyword            A  S  G  A  R  D  A  S  G  A  R  D  A  S  G  A
Key Numbers (2)    0  18 6  0  17 3  0  18 6  0  17 3  0  18 6  0
(1) - (2) mod 26   17 0  6  13 0  17 14 10 8  18 2  14 12 8  13 6
Decrypted          R  A  G  N  A  R  O  K  I  S  C  O  M  I  N  G
```

Decoding the message yields

```
Ragnarok is coming
```

1.2 One-Time Pad

The *one-time pad* is a special case of the Vigenere cipher where the key sequence is

- never re-used,
- at least as long as the plaintext,

- "unrelated to the plaintext," and
- "totally random," in the sense that each number 0 through 25 is equally likely in each position of the key.

Essentially, the way the one-time pad functions is very similar to the Vigenere cipher, except that the key sequence must not be generated using a keyword[1].

In any case, we'll revisit this section later – it's important to be precise when talking about what "unrelated to the plaintext" and "totally random" means. We'll also see, later on, that this has a property known as *perfect secrecy*, which means that the security of the one-time pad can be mathematically guaranteed.

[1]The issue with this is that words won't have the property that each letter is equally likely.