Vigenere cipher (vector shift cipher)

See Section 2.3 of our book for a full description of the Vigenere cipher.

This cipher was long believed by many (until early 20th) to be secure against ciphertext only attacks (more on the classification of attacks shortly).

Example 25. Let us encrypt $HOLIDAY$ using a Vigenere cipher with key BAD (i.e. $1, 0, 3$).

	H	O	L	I	D	A	Y
$+$	B	A	D	B	A	D	B
$=$	I	O	O	J	D	D	Z

Hence, the ciphertext is $IOOJDDZ$.

Example 26. (bonus challenge!) You find a post-it with the following message:

```
NIVU QV JR DTTS ULIFI FOI KIVVF
```

Can you make any sense of it? Word on the street is that Alice was using a Vigenere cipher with key of size 3 with last letter `R`.

(To collect a bonus point, send me an email before next class with the plaintext and how you found it.)

If you can decipher the above message, you have successfully mounted a **ciphertext only attack**.

That is, just knowing the encrypted message, we were able to decrypt it (and discover the key that was used). This is the worst kind of vulnerability.

Attacks

So far, we considered the weakest kind of attack only: namely, a **ciphertext only attack**. And, even then, the historical ciphers prove to be terribly insecure.

However, we need to also worry about attacks where our enemy has additional insight.

- In a **known plaintext attack**, the enemy somehow has knowledge of a plaintext-ciphertext pair (m, c).
- In a **chosen plaintext attack**, the enemy can, herself, compute $c = E(m)$ for a chosen plaintext m ("gained some sort of access to our encryption device").
- In a **chosen ciphertext attack**, the enemy can, herself, compute $m = D(c)$ for a chosen ciphertext c ("gained some sort of access to our decryption device").

There exist many variations of these. Sometimes, the attacker can make several choices (maybe even adaptively), sometimes she only has partial information.

Example 27. Alice sends the ciphertext $BKNDKGBQ$ to Bob. Somehow, Eve has learned that Alice is using the Vigenere cipher and that the plaintext is $ALLCLEAR$. Next day, Alice sends the message $DNFFQGE$. Crack it and figure out the key that Alice used! (What kind of attack is this?)

Armin Straub
straub@southalabama.edu

Solution. This is a known plaintext attack.

Since $m+k=c$ (to be interpreted characterwise, modulo 26, and with k repeated as necessary), we can find k simply as $k=c-m$.

For instance, since A (value 0!) got encrypted to B, the first letter of the key is B.

c			B	K	N	D	K	G	B	Q
m		$-$	A	L	L	C	L	E	A	R
k		$=$	B	Z	C	B	Z	C	B	Z

We conclude that the key is $k=BZC$.

Note. Now, we can decrypt any future message that Alice sends using this key. For instance, we easily decrypt $DNFFQGE$ to $CODEREDD$ (using $m=c-k$).

All of the historical ciphers we have seen, including the substitution cipher that we will discuss shortly, fall apart completely under a known plaintext attack.

Euler's theorem

Example 28. Compute $3^{1003} \pmod{101}$.

Solution. Since 101 is a prime, $3^{100} \equiv 1 \pmod{101}$ by Fermat's little theorem.

Because $3^{100} \equiv 3^0 \pmod{101}$, this enables us to reduce exponents modulo 100.

In particular, since $1003 \equiv 3 \pmod{100}$, we have $3^{1003} \equiv 3^3 = 27 \pmod{101}$.

Fermat's little theorem is a special case of Euler's theorem :

Theorem 29. (Euler's theorem) If $n \geqslant 1$ and $\gcd(a,n)=1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. Euler's theorem can be proved along the lines of our earlier proof of Fermat's little theorem. The only adjustment is to only start with multiples ka where k is invertible modulo n. There are $\phi(n)$ such residues k, and so that's where Euler's phi function comes in. Can you complete the proof? □

Example 30. What are the last two (decimal) digits of 3^{7082}?

Solution. We need to determine $3^{7082} \pmod{100}$. $\phi(100) = \phi(2^2 5^2) = \phi(2^2)\phi(5^2) = (2^2-2^1)(5^2-5^1) = 40$.

Since $\gcd(3,100)=1$ and $7082 \equiv 2 \pmod{40}$, Euler's theorem shows that $3^{7082} \equiv 3^2 = 9 \pmod{100}$.

Binary exponentiation

Example 31. Compute $3^{25} \pmod{101}$.

Solution. Fermat's little theorem is not helpful here.

Instead, we do **binary exponentiation**:

$3^2 = 9$, $3^4 = 81 \equiv -20$, $3^8 \equiv (-20)^2 = 400 \equiv -4$, $3^{16} \equiv (-4)^2 \equiv 16$, all modulo 101

$25 = 16+8+1$ [Every integer $n \geqslant 0$ can be written as a sum of distinct powers of 2 (in a unique way).]

Hence, $3^{25} = 3^{16} \cdot 3^8 \cdot 3^1 \equiv 16 \cdot (-4) \cdot 3 = -192 \equiv 10 \pmod{101}$.

Example 32. (extra practice) Compute $2^{20} \pmod{41}$.

Solution. $2^2 = 4$, $2^4 = 16$, $2^8 = 256 \equiv 10$, $2^{16} \equiv 100 \equiv 18$. Hence, $2^{20} = 2^{16} \cdot 2^4 \equiv 18 \cdot 16 = 288 \equiv 1 \pmod{41}$.

Or: $2^5 = 32 \equiv -9 \pmod{41}$. Hence, $2^{20} = (2^5)^4 \equiv (-9)^4 = 81^2 \equiv (-1)^2 = 1 \pmod{41}$.

Comment. Write $a = 2^{20} \pmod{41}$. It follows from Fermat's little theorem that $a^2 = 2^{40} \equiv 1 \pmod{41}$. The argument below shows that $a \equiv \pm 1 \pmod{41}$ [but we don't know which until we do the calculation].

The equation $x^2 \equiv 1 \pmod{p}$ is equivalent to $(x-1)(x+1) \equiv 0 \pmod{p}$ [b/c $(x-1)(x+1) = x^2-1$]. Since p is a prime and $p \mid (x-1)(x+1)$, we must have $p \mid (x-1)$ or $p \mid (x+1)$. In other words, $x \equiv \pm 1 \pmod{p}$.