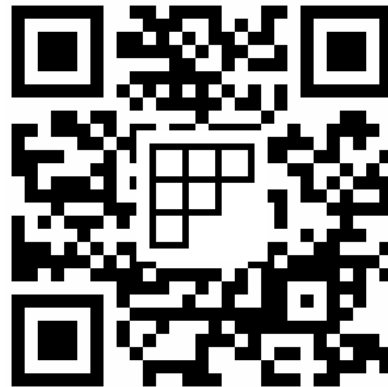


Week 5, lecture 2:
Applications to cryptography
MA180/185/190 Algebra

Angela Carnevale



Applications: cryptography

Affine ciphers: decoding

If we happen to know the affine transformation f_E used to encrypt a message (and the alphabet used), we can decode a message by inverting the function f_E and applying the inverse transformation to the ciphertext.

We know that $f_E(x) = ax + b$, so to recover x we write:

$$ax + b = y \quad \text{so} \quad x = a^{-1}(y - b) = a^{-1}y - a^{-1}b$$

\uparrow
letter in the cipher-text (so what needs to be decoded)

Note.

- ▶ Here we used the fact that a in the affine transformation is invertible in \mathbb{Z}_{26} .
- ▶ In general, one can use alphabets containing more symbols, upper and lower case letters, numbers etc.

Affine ciphers: decoding

Example (continued). The following message was encrypted using the affine transformation in the previous example: WDAZ

What's the plaintext?

Recall $f_E(x) = 3x + 11$

if $y = 3x + 11$ then $x = 3^{-1}(y - 11) = 3^{-1}y - 3^{-1} \cdot 11$

Need: $3^{-1} \in \mathbb{Z}_{26}$? Note: $3 \cdot 9 = 27 \equiv 1 \pmod{26}$ so $9 = 3^{-1}$

$f_D(x) = 9 \cdot x - 9 \cdot 11 = 9 \cdot x + 5$ (since the coefficients are mod 26)

W = 23	$\xrightarrow{f_D(x)}$	$9 \cdot 23 + 5 = 212 \equiv 4 \pmod{26}$	D
D = 4		$9 \cdot 4 + 5 = 41 \equiv 15 \pmod{26}$	O
A = 1		$9 \cdot 1 + 5 \equiv 14 \pmod{26}$	N
Z = 0		$9 \cdot 0 + 5 \equiv 5 \pmod{26}$	E



New challenge: a ciphertext

We receive the following ciphertext:

OT WOZMZ

LZII UXSZ UZPXUTSJ WOTR NZRRFJZ

(here the space between words was maintained).

We know it was encrypted via an affine transformation, but we don't know the key.

Can you decode the message?

Hint. Can you guess what 2-word letter could open such message?

Public key cryptography

A **public-key cryptosystem** is one in which each user publishes numerical information which enables any other user to encode messages, but does not give away enough information to allow anyone else to decode them.

A famous such system is the so-called **RSA cryptosystem**. It is based on two main mathematical facts/ideas:

- ▶ While it's easy to multiply numbers together, it is hard to find prime factors of very large numbers¹
- ▶ Euler's totient theorem

¹Try it out! Can you easily tell what are the prime factors of **123276509**?

Introduction to RSA

To use this system, each person chooses a pair of (very) large primes p and q and then calculates $n = pq$.

After choosing p and q , we can easily calculate $\phi(n)$. Indeed, since $n = pq$, $\phi(n) = (p - 1)(q - 1)$.

While keeping $\phi(n)$ secret, we choose a second integer e , coprime to $\phi(n)$. The pair of numbers (n, e) is our **public key**. This information is made public (e.g. added to our webpage).

Anyone wishing to send us a message can use the pair of numbers (n, e) to encode a message that we (and nobody else!) will be able to decode. The function used in this case is the following function from \mathbb{Z}_n to \mathbb{Z}_n :

$$x \mapsto x^e.$$

Decoding

To decode a message of this form, the receiver uses their private key (and Euler's theorem!) as follows.

First, note that since e is coprime to $\phi(n)$, it has an inverse modulo $\phi(n)$, that is d such that $ed \equiv 1 \pmod{\phi(n)}$. This tells us that there is some k such that

$$ed = k \cdot \phi(n) + 1$$

So we can recover x by computing

$$(x^e)^d \equiv x^{ed} \equiv x^{k\phi(n)} \cdot x \equiv x \pmod{n},$$

where we used that, thanks to Euler's theorem, $x^{k\phi(n)} \equiv 1 \pmod{n}$

Example

Alice chooses primes $p = 7$ and $q = 29$. She then computes $n = p \cdot q = 7 \cdot 29 = 203$ and $\phi(n) = \phi(p \cdot q) = 6 \cdot 28 = 168$.

To complete her **public key** she now needs an integer e such that $0 < e < 168$ and that is coprime to 168.

Alice's public key is $(n, e) = (203, 5)$.

To be able to decrypt any messages sent to her, she still needs to compute her (private) decryption key. This is $e^{-1} \bmod 168$.

That is, she needs d such that $e \cdot d \equiv 1 \bmod 168$


Noting that $5 \cdot 101 = 505 = 3 \cdot 168 + 1$, we get that $d = 5^{-1} = 101 \bmod 168$

So to decode any message sent to her and encrypted via (n, e) , Alice will

use the decoding function $x \mapsto x^d \pmod{203}$

Example

Bob would like to send Alice the message "53".

Bob  use Alice's encoding function
 $\leadsto 53 \mapsto 53^5 \pmod{203}$. This gives him 65
so "65" is the ciphertext he sends on.

Now Alice gets the ciphertext 65 and decodes it by taking the 101-power:

$$65^{101} \equiv \underline{\underline{53}} \pmod{203}$$

\uparrow

Alice recovered the original ciphertext!

