Lecture 11: Cryptology

Cryptology

Cryptology is the science of building and breaking codes. It consist of **cryptography**, the creation of codes and **cryptanalysis**, the theory of cracking codes. The two subfields are obviously related like differentiation and integration are related in calculus.

A related field is the theory of **error correcting codes**. But there the purpose is different. The goal of the later is also to find codes which make the transmissions more secure but in the sense that minor data corruption or loss can be recovered or corrected.

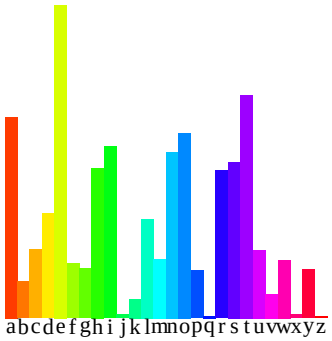
What kind of mathematics is involved? The theory has ties with **probability theory**. Especially in the code breaking part **statistical methods** are useful. Many codes are based on **number theory** like RSA and Diffie-Hellman. Also there, since the numbers are so large, one often refers to probabilistic methods. Then there are combinatorial which come into play when looking at the complexity of codes. Especially in code breaking like with plain text attacks. **Algebraic geometry** has entered through examples like **elliptic curve cryptosystems**. In general, **algebra** enters if algebraic objects like number fields are used. New branches like **quantum cryptology** use analysis like Fourier theory.

Substitution ciphers

1) **Cesar ciphers** permute the alphabet. Examples:

Cesar:	shift three to the left	F becomes C for example
Augustus:	shift to the right	F becomes G.
Atbash:	reflect	B becomes Y and Y becomes B.
Rot13:	move to middle	A Becomes N and N becomes A.

First known attacks using frequency analysis Al Kindi in 9'th century.



2) **Polyalaphabetic ciphers** permute with different alphabets. Examples:

Alberti	Random change of alphabet indicating switch
Trithemius	Deterministic change of alphabet
Viginere	Using key
Enigma	Using key and deterministic alphabet change overlapped with Cesar
Hill Cipher	Use matrices to permute

Block ciphers

Cut text into larger chunks and scramble them. Examples:

DES	Data Encryption Standards 1973
Triple DES	Used for some electronic payments, 1998

Public Key Cyphers

Depends often on Number theoretical mathematical difficulties like factoring integers.

Diffie-Hellman Key exchange	1976 (1974 at GCHQ in England)
RSA encryption	1978 (1973 at GCHQ in England)

The RSA method allows Ana to submit messages to Bob on a public channel which a third party Eve can not read.

Ana publishes a **RSA pair**: (n, a) into the public. The factorization $n = pq$ is secret and $a < (p-1)(q-1)$ is such that there exists b with $ab = 1 \bmod (p-1)(q-1)$. Bob sends a secrete message to Ana by transmitting

$$y = x^a \bmod n \ .$$

Ana can read the email by computing

$$y^b \bmod n \ .$$

The key is public. Still, one can not read the messages unless a hard mathematical problem, the factorization of n is solved.

Diffie Hellman method allows Ana and Bob to exchange keys on a public channel which a third party Eve can not read.

A prime p and primitive root a are given and public. A primitive root is a number for which a^k generates all numbers different from 0 modulo p. Its a number for which the "log" exists.

Ana choses a secret number x and publishes $u = a^x \bmod p$.
Bob choses a secret number y and publishes $v = a^y \bmod p$.
Ana can compute $v^x = a^{xy}$ and Bob can compute $v^y = a^{yx}$ (always modulo p) But Eve, the eves dropper can not get x, y from u, v.