The topic of our first meeting is cryptography - defined as the practice and study of techniques for secure communication in the presence of third parties called adversaries. It is a vast topic which can be studied from many angles, as there are many technical but also social aspects to consider - of course as mathematicians most of us are interested in the mathematical aspects.

In our meeting we would like to initiate a discussion - but without following a prescribed direction. After the introductory talk it is up to the participants where this is taken.

Any contribution is welcome, be it a specific question, a worked out example, a technical detail that you find interesting, a specific algorithm that you like, a mathematical fact that is surprising, considerations about society and security,...
It doesn't have to be perfect, simply let your curiosity and creativity lead you.

Don't worry, if you don't know much about cryptography or if you don't know where to start. Here are som suggestions:

(a) What is the difference beween smmetric and asymmetric encryption?

(b) Can you explain your favourite (historic or modern) encryption method (e.g. Viginère cipher, Substitution cipher, shift cipher, transposition cipher...)? With this method, can you encrypt a message for the other participants that they can try to decrypt?
`http://www.cs.trincoll.edu/~crypto/historical/`

(c) How would you define that an encryption scheme is secure?

(d) What is the deal with the enigma machine?

(e) Identify the encryption schemes: For each pair of plaintext and ciphertext find our which method f encryption was used and write down the key that was used.

- Plaintext: NEVERTRUSTINSECURITYBYOBSCURITY
  Ciphertext: ARIREGEHFGVAFRPHEVGLOLBOFPHEVGL
- Plaintext: THISISASECRETMESSAGE
  Ciphertext: GSRHRHZHVXIVGNVHHZTV
- Plaintext: GOOD
  Ciphertext: OVUA

(f) Here is a cipher text encrypted with Viginère Cipher, all spaces and punctuation removed. Decrypt it using an tool you like.

XUKW LGEE YINN WBVL BWKU VXUC XLQY FJSH NHNV PRCW
GQRP GMAA SHTP VHIO TSJU IGJI JGFS QVFQ QRMM AFIE
IEEV IAEV LRXB VSBN WNUC BWWR GWRX IECP BHXU GQNT
INXE VNEO NINP HNTI DWMG GEON IGQT RTJB TQNH VRSY
RPGL CRNN CFKW NPHG JYFV SRXI AIYR UWGJ IFGG EGXX
GCBH XUKW PKTU GVCN ELKR TCVB WRQY MGJX UGQP CROG
EYQX BHJH PFHV RBYT YGEF GJBT KRVE OQYG VLVU EAEM
RPXF VYSH JBTX UGVR UXBH XUKW PQYE UIVP XUGV ROEV
PHRT SSVL RESH TWRY IJKP YHSP WWBP QBTI RNEO QVNV
ISQV ZUSS UIPW VVVC GJEG EEAP SGDI OTSX GROA WHEL
NUMZ RPRV IPJR VSYR

(g) What is the "factorisation problem" in crptography? Here is a nice number theory exercise in this context:

Assume $N = pq$ where p and q are distinct odd prime numbers.

- If $d \equiv e^{-1} \mathrm{mod} \phi(N)$ show $ed - 1$ is even.
- If $\gcd(m, N) \equiv 1$, what is $m^{ed-1} \mathrm{mod} N$?

- Let $ed - 1 = 2^n L$, with $n \in \mathbb{N}$ and L odd. If m has the property $m^L \not\equiv \pm 1 \mathrm{mod} N$ and $m^{2L} \equiv 1 \mathrm{mod} N$, how can ou find the factors of N?

(h) What is the concept of zero-knowledge? How much data do we have to share in order to only extract a specific piece of data?
`https://mathoverflow.net/questions/22624/example-of-a-good-zero-knowledge-proof?rq=1`
`https://mathoverflow.net/questions/236473/zero-knowledge-proof-of-equality`

(i) What is elliptic curve cryptography?
`https://crypto.stanford.edu/cs355/18sp/lec14.pdf`

(j) Is it possible to determine how secure a ciphering method is?
`https://www.quantamagazine.org/how-the-evercrypt-library-creates-hacker-proof-cryptography-2019`

(k) What is "indistinguishability obfuscation"?
`https://www.quantamagazine.org/a-new-design-for-cryptographys-black-box-20150902/`

(l) Cryptography in the age of quantum computing
`https://www.quantamagazine.org/quantum-secure-cryptography-crosses-red-line-20150908/`