Symmetric ciphers

- encryption algorithm $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$
- decryption algorithm $D : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

st. $\forall k \in \mathcal{K}$, and $\forall m \in \mathcal{M}$, $D(k, E(k, m)) = m$

- same key $k$ to encrypt and decrypt
- the key $k$ is secret: only known to Alice and Bob

Examples: One-time pad, DES, AES, ...
Asymmetric ciphers

- key generation algorithm: $G: \rightarrow \mathcal{K} \times \mathcal{K}$
- encryption algorithm $E: \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$
- decryption algorithm $D: \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

st. $\forall (sk, pk) \in G$, and $\forall m \in \mathcal{M}$, $D(sk, E(pk, m)) = m$

- the decryption key $sk$ is secret (only known to Bob). The encryption key $pk$ is known to everyone. And $sk \neq pk$

Examples: RSA, ElGamal, Diffie-Hellman, ...
Digital signatures

- Key generation algorithm: $G : \rightarrow \mathcal{K} \times \mathcal{K}$
- Signing algorithm $S : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{S}$
- Verification algorithm $V : \mathcal{K} \times \mathcal{S} \rightarrow \{\top, \bot\}$

s.t. $\forall (sk, vk) \in G$, and $\forall m \in \mathcal{M}$, $V(vk, S(sk, m)) = \top$

- The signing key $sk$ is secret (only known to Alice). The verification key $vk$ is known to everyone. And $sk \neq vk$

Examples: RSA based, ElGamal based, Schnorr, ...
Hashes

- hash algorithm $H : \mathcal{M} \rightarrow \mathcal{D}$

- **preimage resistant**: given a digest $d$, it is computationally infeasible to find any message $m$ such that $H(m) = d$

- **collision resistance**: it is hard to find two different messages $m_1 \neq m_2$ such that $H(m_1) = H(m_2)$

- applications: commitment schemes, signature schemes, MACs, key derivation algorithms, ...

Examples: MD5, SHA-1, ...
Many more crypto primitives

- Message Authentication Codes (MACs)
- Zero Knowledge Proofs (ZKPs)
- Fully Homomorphic Encryption (FHE)
- ...

...
Historical ciphers

Myrto Arapinis
School of Informatics
University of Edinburgh
Rail fence cipher

- shared secret key $k \in \mathbb{N}$

- **Encryption**: plaintext written in columns of size $k$. The ciphertext is the concatenation of the resulting rows.

  $k=6$

  $$m = \text{THIS COURSE AIMS TO INTRODUCE YOU TO THE PRINCIPLES AND TECHNIQUES OF SECURING COMPUTERS}$$

  $$c = \text{TOAOOY RLDN C THUI DOTIE IOUCEIRMIUHNSSTQFROSTRSSNC EC EU IMS E TET IACESNPC TR OPPNHSEGUQ}$$

- **Decryption**: ciphertext written in rows of size $\frac{|c|}{k}$
Rail fence cipher

- shared secret key $k \in \mathbb{N}$
- Encryption: plaintext written in columns of size $k$. The ciphertext is the concatenation of the resulting rows.

$k=6$

$m = \text{THIS COURSE AIMS TO INTRODUCE YOU TO THE PRINCIPLES AND TECHNIQUES OF SECURING COMPUTERS}$

<table>
<thead>
<tr>
<th>T</th>
<th>O</th>
<th>A</th>
<th>O</th>
<th>Y</th>
<th>R</th>
<th>L</th>
<th>D</th>
<th>N</th>
<th>C</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>U</td>
<td>I</td>
<td>D</td>
<td>O</td>
<td>T</td>
<td>I</td>
<td>E</td>
<td>I</td>
<td>O</td>
<td>U</td>
</tr>
<tr>
<td>I</td>
<td>R</td>
<td>M</td>
<td>I</td>
<td>U</td>
<td>U</td>
<td>H</td>
<td>N</td>
<td>S</td>
<td>T</td>
<td>Q</td>
</tr>
<tr>
<td>S</td>
<td>S</td>
<td>S</td>
<td>N</td>
<td>C</td>
<td>E</td>
<td>C</td>
<td>E</td>
<td>U</td>
<td>I</td>
<td>M</td>
</tr>
<tr>
<td>E</td>
<td>T</td>
<td>E</td>
<td>T</td>
<td>I</td>
<td>A</td>
<td>C</td>
<td>E</td>
<td>S</td>
<td>N</td>
<td>P</td>
</tr>
<tr>
<td>C</td>
<td>T</td>
<td>R</td>
<td>O</td>
<td>P</td>
<td>P</td>
<td>N</td>
<td>H</td>
<td>S</td>
<td>E</td>
<td>G</td>
</tr>
</tbody>
</table>

$c = \text{TOAOOY RLDN C THUI DOTIE IOUCEIRMIUUHNSSTQFRORSSNC EC EU IMS E TET IACESNPC TR OPPNHSEGUQ}$

- Decryption: ciphertext written in rows of size $\frac{|c|}{k}$

But small key space size: $k < |c| \Rightarrow$ brute force attack!!
Substitution cipher

- shared secret: a permutation \( \varpi \) of the set of characters

\[
\varpi = \begin{array}{cccccccccccccccccccc}
    a & \mapsto & q & b & \mapsto & w & c & \mapsto & e & d & \mapsto & r & e & \mapsto & t & f & \mapsto & y & g & \mapsto & u & h & \mapsto & i & i & \mapsto & o & j & \mapsto & m & k & \mapsto & a & l & \mapsto & s \\
    m & \mapsto & d & n & \mapsto & f & o & \mapsto & g & p & \mapsto & h & q & \mapsto & j & r & \mapsto & k & s & \mapsto & l & t & \mapsto & z & u & \mapsto & x & v & \mapsto & c & w & \mapsto & v & x & \mapsto & b \\
    y & \mapsto & n & z & \mapsto & p
\end{array}
\]

- Encryption: apply \( \varpi \) to each character of the plaintext.

\[
E(\varpi, m_1 \ldots m_n) = \varpi(m_1) \ldots \varpi(m_n)
\]

- Decryption: apply \( \varpi^{-1} \) to each character of the plaintext.

\[
D(\varpi, c_1 \ldots c_n) = \varpi^{-1}(c_1) \ldots \varpi^{-1}(c_n)
\]
m = THIS COURSE AIMS TO INTRODUCE YOU TO THE PRINCIPLES AND TECHNIQUES OF SECURING COMPUTERS AND COMPUTER NETWORKS WITH FOCUS ON INTERNET SECURITY. THE COURSE IS EFFECTIVELY SPLIT INTO TWO PARTS. FIRST INTRODUCING THE THEORY OF CRYPTOGRAPHY INCLUDING HOW MANY CLASSICAL AND POPULAR ALGORITHMS WORK E.G. DES, RSA, DIGITAL SIGNATURES, AND SECOND PROVIDING DETAILS OF REAL INTERNET SECURITY PROTOCOLS, ALGORITHMS, AND THREATS, E.G. IPSEC, VIRUSES, FIREWALLS. HENCE, YOU WILL LEARN BOTH THEORETICAL ASPECTS OF COMPUTER AND NETWORK SECURITY AS WELL AS HOW THAT THEORY IS APPLIED IN THE INTERNET. THIS KNOWLEDGE WILL HELP YOU IN DESIGNING AND DEVELOPING SECURE APPLICATIONS AND NETWORK PROTOCOLS AS WELL AS BUILDING SECURE NETWORKS.

c = ZIOL EGXKLT QODL ZG OFZKGRXET NGX ZG ZIT HKOFEOHSTL QFR ZTEIFOJXTL GY LTEXKOFU EGDHXZTKL QFR EGDHXZTK FTZVGKAL VOZI YGEXL GF OFZTKFTZ LTEXKOZN. ZIT EGXKLT OL TYYTEZOCTSN LHSOZ OFZG ZVG HQKZL. YOKLZ OFZKGRXEOFU ZIT ZITGKN GY EKHZGUKQHIN OFESXROFU IGV DQFN ESLLOEQS QFR HGHXSQK QSUGKOZIDL VGKA T.U. RTL, KLQ, ROOUQZS LOUFQZXKTL, QFR LTEGFR HKGCOROFU RTZQOSL GY KTQS OFZTKFTZ LTEXKOZN HKGZGEGSL, QSUGKOZIDL, QFR ZIKTQZL, T.U. OHLTE, COKXLTL, YOKTVQSSL. ITFET, NGX VOSS STQKF WGZI ZITGKTZOEQS QLHTEZL GY EGDHXZTK QFR FTZVGKA LTEXKOZN QL VTSS QL IGV ZIQZ ZITGKN OL QHHSOTR OF ZIT OFZTKFTZ. ZIOL AFGVSTRUT VOSS ITSH NGX OF RTLOUFOFU QFR RTCTSGHOFU LTEXKT QHHSOEOQZOGFL QFR FTZVGKA HKGZGEGSL QL VTSS QL WXOSROFU LTEXKT FTZVGKAL.
Breaking the substitution cipher

- Key space size: $|K| = 26! \approx 2^{88}$
  \[\Rightarrow\text{brute force infeasible!}\]
- Exploit regularities of the language
  - Use frequency of letters in English text:
    \(e > t > a\)
  - Use frequency of digrams in English text:
    \(th > he > in\)
  - Use frequency of trigrams in English text:
    \(the > and > ing\)
- Use expected words
Breaking the substitution cipher

- Key space size: $|\mathcal{K}| = 26! (\approx 2^{88}) \Rightarrow$ brute force infeasible!
Breaking the substitution cipher

- Key space size: $|\mathcal{K}| = 26! \approx 2^{88}$ ⇒ brute force infeasible!

- Exploit regularities of the language
  - Use frequency of letters in english text
    
    $e > t > a > o$
  
  - Use frequency of digrams in english text
    
    $th > he > in > er$
  
  - Use frequency of trigrams in english text
    
    $the > and > ing$

- Use expected words
Breaking the substitution cipher: example

c = ZIOL EGXKLT QODL ZG OFZKGRXET NGX ZG ZIT HKOFEOHSTL QFR ZTEIFOJXTL GY LTEXKOFU EGDHXZTCL QFR EGDHXZTK FTZVGKAL VOZI YGEXL GF OFZTKFTZ LTEXKOZN. ZIT EGXKLT OL TYYTEZOCTSN LHSOZ OFZG ZVG HQKZL. YOKLZ OFZKGRXEOFU ZIT ZITGKN GY EKNHZGUKQHIN OFESXROFU IGV DQFN ESQLLOEQS QFR HGHXSQK QSUGKOZIDL VGKA T.U. RTL, KLQ, ROUOZQS LOUFQZXKTL, QFR LTEGFR HKGCOROFU RTZQOSL GY KTQS OFZTKFTZ LTEXKOZN HKGZGEGSL, QSUGKOZIDL, QFR ZIKTQZL, T.U. OHLTE, COKXLTL, YOKTVQSSL. ITFET, NGX VOSS STQKF WGZI ZITGKTZOEQS QLHTEZL GY EGDHXZTK QFR FTZVGKA LTEXKOZN QL VTSS QL IGV ZIQZ ZITGKN OL QHHSOTR OF ZIT OFZTKFTZ. ZIOL AFGVSTRUT VOSS ITSH NGX OF RTLHFOFU QFR RTCTSGHOFU LTEXKT QHHSOEQZOGFL QFR FTZVGKA HKGZGEGSL QL VTSS QL WXOSROFU LTEXKT FTZVGKAL.
Breaking the substitution cipher: example

\[ c = \text{TIOLEGXKLE QODL TG OFTKGRXEE NGX TG TIE HKOFEOHSEL QFR TEEIFOJXEL GY LEEXKOFU EGDHXTEKL QFR EGDHXTEK FETVGGKAL VOTI YGEXL GF OFTEKFET LEEXKOTN. TIE EGXKLE OL EYYEETOCESN LHSOT OFTG TVG HQKTL. YOKLT OFTKGRXEOFU TIE TIEGKN GY EKNHTGUKQHIN OFESXROFU IGV DQFN ESQLOEQS QFR HGHSQK QSUGKOTIDL VGKA E.U. REL, KLQ, ROUOTQS LOUFQTXKEL, QFR LEELGR HKGCOROFU RETQOSL GY KEQS OFTEKFET LEEXKOTN HKGTGEGSL, QSUGKOTIDL, QFR TIEOQTL, E.U. OHLEE, COKXLEL, YOKEVQSSL. IEFE, NGX VOSS SEQKF WGTI TIEGKETOEQS QLHEETL GY EGDSXTEK QFR FETVGGKAL LEEXKOTN QL VESS QL IGV TIEQTL TIEGKN OL QHHSOER OF TIE OFTEKFET. TIOLEAGVSERUE VOSS IESH NGX OF RELOUOFU QFR RECSEGHOFU LEEXKE QHHSOEQTOGFL QFR FETVGGKA HKGTGEGSL QL VESS QL WXOSRQFU LEEXKE FETVGGKAL. ]

Most common letters in c: t \(>\) z \(>\) ...
Breaking the substitution cipher: example

\[ c = \text{THOL EGXKLE QODL TG OFTKGRXEE NGX TG THE HKOFEOHS} \text{EL QFR TEEHFOJXEL GY LEEXKOFU EGDHXTEKLF QFR EGDHXTEK FETVGBKAL VOTH YGEXL GF OFTEKFET LEEXKOTN. THE EGXKLE OL EYYEETOCESN LHSOT OFTG TVG HQKTL. YOKLT OFTKGRXEOFU THE THEGKN GY EKNHTGU} \text{KQHHN OFESXROFU HGV DQFN ESQLLOEQS QFR HGHXSOQK QSUGKOTHDL VGKA E.U. REL, KLQ, ROUQTQS LOUFQTXKEL, QFR LEEGFR HKGCOROFU RETQOSL GY KEQS OFTEKFET LEEXKOTN HKGTGEGSL, QSUGKOTHDL, QFR THKEQTL, E.U. OHLEE, COKXLEL, YOKEVQSSL. HEFEE, NGX VOSS SEQKF WGTTH THEGKETOEQS QLHEETL GY EGDHXTEK QFR FETVGBKAL LEEXKOTN QL VESS QL HGV THQT THEGKN OL QHHSOER OF THE OFTEKFET. THOL AFGVSERUE VOSS HESH NGX OF RELOUFOFU QFR RECESGHOFU LEEXKE QHHSOEQTOGFL QFR FETVGBKAL HKGTGEGSL QL VESS QL WXOSROFU LEEXKE FETVGBKAL.} \]

Most common digrams in c: of > zi > …

t↦z suggests h↦i
Breaking the substitution cipher: example

\[c = \text{THIL EGXKLE QIDL TG INTKGRXEE NGX TG THE HKINEIHSEL QNR TEEHNIJXEL GY LEEXKINU EGDHXTEKL QNR EGDHXTEK NETVGKAL VITH YGEXL GN INTEKNET LEEXKITN. THE EGXKLE IL EYYEETICESN LHSIT INTG TVG HKKTL. YIKLT INTKGRXEINU THE THEGKN GY EKNHTGUKQHHN INESXRINU HGV DQNN ESLQLEQS QNR HGHXSQK QSUGKITHDL VGKA E.U. REL, KLQ, RIUITQS LIUNQTXKEL, QNR LEEGNR HKGCIRINU RETQISL GY KEQS INTEKNET LEEXKITN HKGTGEGSL, QSUGKITHDL, QNR THKEQTL, E.U. IHLEE, CIKXLEL, YIKEVQSSL. HENEE, NGX VISS SEQKN WGTH THEGKETIEQS QLHEETL GY EGDHXTEK QNR NETVGKA LEEXKITN QL VEES QL HGV THQT THEGKN IL QHHSIER IN THE INTEKNET. THIL ANGVSERUE VISS HESH NGX IN RELIUNINU QNR RECESGHINU LEEXKE QHHSIEQTIGNL QNR NETVGKA HKGTGEGSL QL VEES QL WXISRINU LEEXKE NETVGKAL.}\]

Most common digrams in c: of \(\succ\) zi \(\succ\) \ldots

we guess in \(\mapsto\) of
Breaking the substitution cipher: example

We identify in \( c \) the word INTEKNET suggests \( r \mapsto k \)
Breaking the substitution cipher: example

c = THIS EGXRSE QIDS TG INTRGRXEE NGX TG THE HRINEIHSES QNR TEEHNIJXES GY SEEXRINU EGDHXTER EGDHXTER NETVGRAS VITH YGEXS GN INTERNET SEEXRITN. THE EGXRSE IS EYYEETICESN SHSIT INTG TVG HQRTS. YIRST INTRGRXEINU THE THEGRN GY ERNHTGURQHHN INESXRINU HGV DQNN ESQSSIEQS QNR HGHXSRQ QSUGRITHDS VGRA E.U. RES, RSQ, RIVITQS SIUNQTXRES, QNR SEEGNR HRGCRIRINU RETQISS GY REQS INTERNET SEEXRITN HRGTGEGSS, QSUGRITHDS, QNR THREIQTS, E.U. IHSEE, CIRXSES, YIREVQSSS. HENEE, NGX VISS SEQRN WGTH THEGRETIEQS QSHEETS GY EGDHXTER QNR NETVGRA SEEXRITN QS VEES QS HGV THQT THEGRN IS QHHSIER IN THE INTERNET. THIS ANGVUSERUE VISS HESH NGX IN RESIUNINU QNR RCESEGHINU SEEXRE QHHSIEQTIGNS QNR NETVGRA HRGTGEGSS QS VEES QS WXISRINU SEEXRE NETVGRAS.

The first word is THIL suggests s→l
Breaking the substitution cipher: example

\[
m = \text{THIS COURSE AIMS TO INTRODUCE YOU TO THE PRINCIPLES AND TECHNIQUES OF SECURING COMPUTERS AND COMPUTER NETWORKS WITH FOCUS ON INTERNET SECURITY. THE COURSE IS EFFECTIVELY SPLIT INTO TWO PARTS. FIRST INTRODUCING THE THEORY OF CRYPTOGRAPHY INCLUDING HOW MANY CLASSICAL AND POPULAR ALGORITHMS WORK E.G. DES, RSA, DIGITAL SIGNATURES, AND SECOND PROVIDING DETAILS OF REAL INTERNET SECURITY PROTOCOLS, ALGORITHMS, AND THREATS, E.G. IPSEC, VIRUSES, FIREWALLS. HENCE, YOU WILL LEARN BOTH THEORETICAL ASPECTS OF COMPUTER AND NETWORK SECURITY AS WELL AS HOW THAT THEORY IS APPLIED IN THE INTERNET. THIS KNOWLEDGE WILL HELP YOU IN DESIGNING AND DEVELOPING SECURE APPLICATIONS AND NETWORK PROTOCOLS AS WELL AS BUILDING SECURE NETWORKS.}
\]

Going back to letter frequency and a few more guesses!!
Vigenere cipher

- shared secret key: a word $w$ over the english alphabet

Encryption: break the plaintext $m = m_1 \ldots m_n$ in blocks, and encrypt each block as follows

$m_i + 1 \ldots m_{i+1} \oplus w \oplus w \oplus \ldots \oplus w \pmod{26}$

$\downarrow \uparrow$

$c_{i+1} \ldots m_{i+1} \oplus w \oplus w \oplus \ldots \oplus w \pmod{26}$

$\downarrow \uparrow$

Concatenate the resulting blocks to obtain the ciphertext

Decryption: break the ciphertext $c = c_1 \ldots c_n$ in blocks, and decrypt each block as follows

$c_{i+1} \ldots c_{i+1} \ominus w \ominus w \ominus \ldots \ominus w \pmod{26}$

$\downarrow \uparrow$

$m_{i+1} \ldots m_{i+1} \ominus w \ominus w \ominus \ldots \ominus w \pmod{26}$

$\downarrow \uparrow$

Concatenate the resulting blocks to retrieve the message
Vigenere cipher

- shared secret key: a word \( w \) over the english alphabet
- Encryption: break the plaintext \( m = m_1 \ldots m_n \) in \( \frac{m}{w} \) blocks, and encrypt each block as follows

\[
\begin{align*}
\begin{array}{c}
m_{i+1} \\
+ \ w_1 \\
\end{array} & \quad \ldots \quad \begin{array}{c}
m_{i+|w|} \\
+ \ w_{|w|} \\
\end{array} \\
\begin{array}{c}
m_{i+1} + w_1 \pmod{26} \\
\end{array} & \quad \ldots \quad \begin{array}{c}
m_{i+|w|} + w_{|w|} \pmod{26} \\
\end{array} \\
\begin{array}{c}
c_{i+1} \\
\end{array} & \quad \ldots \quad \begin{array}{c}
c_{i+|w|} \\
\end{array}
\end{align*}
\]

Concatenate the resulting blocks to obtain the ciphertext
Vigenere cipher

- shared secret key: a word $w$ over the English alphabet
- Encryption: break the plaintext $m = m_1 \ldots m_n$ in $\frac{|m|}{|w|}$ blocks, and encrypt each block as follows

\[
\begin{align*}
    m_{i+1} & \quad \ldots \quad m_{i+|w|} \\
    + & \quad \ldots \quad + \\
    w_1 & \quad \ldots \quad w_{|w|} \\
\end{align*}
\]

\[
\begin{align*}
    m_{i+1} + w_1 \pmod{26} & \quad \ldots \quad m_{i+|w|} + w_{|w|} \pmod{26} \\
\end{align*}
\]

$\underbrace{c_{i+1}} \quad \ldots \quad \underbrace{c_{i+|w|}}$

Concatenate the resulting blocks to obtain the ciphertext

- Decryption: break the ciphertext $c = c_1 \ldots c_n$ in $\frac{|m|}{|w|}$ blocks, and decrypt each block as follows

\[
\begin{align*}
    c_{i+1} & \quad \ldots \quad c_{i+|w|} \\
    - & \quad \ldots \quad - \\
    w_1 & \quad \ldots \quad w_{|w|} \\
\end{align*}
\]

\[
\begin{align*}
    c_{i+1} - w_1 \pmod{26} & \quad \ldots \quad c_{i+|w|} - w_{|w|} \pmod{26} \\
\end{align*}
\]

$\underbrace{m_{i+1}} \quad \ldots \quad \underbrace{m_{i+|w|}}$

Concatenate the resulting blocks to retrieve the message
Vigenere cipher: example

\[ w = MACBETH \]

\[ m = WHEN SHALL WE THREE MEET AGAIN IN THUNDERLIGHTNING OR IN RAIN \]

\[ \begin{array}{cccccccccccccccccccccccccccccc}
M & A & C & B & E & T & H & M & A & C & B & E & T & H & \ldots & M & A \\
+ & W & H & E & N & S & H & A & L & L & W & E & T & H & R & \ldots & I & N \\
\end{array} \]

\[ \begin{array}{cccccccccccccccccccccccccccccc}
J & I & H & P & X & B & I & Y & M & Z & G & Y & B & Z & \ldots & V & O \\
\end{array} \]

\[ c = IHGO WAHXL YF XAYQE OFIM HSAKO MG ATUPEIKSUGJVRBUS OT JR KHUN \]
Breaking the Vigenere cipher

Suppose we know the length of the key $w$. Break the ciphertext in $|c|\times|w|$ blocks: $c_1 \ldots c_{|w|} \mid |c| \mid c_{|w|+1} \ldots c_2 \mid |c| \mid c_{|w|+2} \ldots |c| - |w| + 1 \ldots |c|$. For each position in $\{1, \ldots, |w|\}$, consider the characters $c_j \mid |w| + i$ for all $j \in |c| \setminus |w|$. All these characters have been encrypted using the same key character $w_i$. Perform letter frequency analysis on this set of characters.

If the size of $w$ is not known apply Kasiski’s method to narrow the possibilities:

- identify all the sequences of letters of length greater than 4 that occur more than once
- for each such sequence compute the distance between two of its occurrences
- compute the corresponding possible key-length
Suppose we know the length of the key $w$. Break the ciphertext in $\frac{|c|}{|w|}$ blocks:

$$c_1 \ldots c_{|w|} \parallel c_{|w|+1} \ldots c_{2|w|} \parallel \cdots \parallel c_{|c|-|w|+1} \ldots c_{|c|}$$

for each position in $\{1, \ldots, |w|\}$, consider the characters $c_{j|w|+i}$ for all $j \in \frac{|c|}{|w|}$. All these characters have been encrypted using the same key character $w_i$. Perform letter frequency analysis on this set of characters.
Breaking the Vigenere cipher

- Suppose we know the length of the key $w$. Break the ciphertext in $\frac{|c|}{|w|}$ blocks:

$$c_1 \cdots c_{|w|} \parallel c_{|w|+1} \cdots c_{2|w|} \parallel \cdots \parallel c_{|c|-|w|+1} \cdots c_{|c|}$$

for each position in $\{1, \ldots, |w|\}$, consider the characters $c_{j|w|+i}$ for all $j \in \frac{|c|}{|w|}$. All these characters have been encrypted using the same key character $w_i$. Perform letter frequency analysis on this set of characters.

- If the size of $w$ is not known apply Kasiski’s method to narrow the possibilities:
  - identify all the sequences of letters of length greater than 4 that occur more than once
  - for each such sequence compute the distance between two of its occurrences
  - compute the corresponding possible key-length
Rotor machines: the Herbern machine

Rotor machines: the enigma machine

Rotors

Keyboard

Lampboard

Plugboard