Playfair

Playfair is een van de klassieke versleutelingsmethoden. Deze codeertechniek werd in 1854 door Sir Charles Wheatstone uitgevonden, maar draagt de naam van Lyon Playfair die het gebruik ervan promootte. De eenvoud in gebruik en de veiligheid van deze polygrafische substitutieversleuteling — vergeleken met andere substitutiecoderingen zoals Vigenère — maakten van Playfair een populaire versleutelingsmethode. In een 19 pagina's lang pamflet uit 1914 van de hand van Joseph O. Mauborgne wordt voor het eerst de oplossing van een Playfaircodering gegeven.

Sir Charles Wheatstone (Barnwood, 6 februari 1802 – Parijs, 9 oktober 1875)

Voor het coderen en decoderen van berichten wordt bij Playfair gebruik gemaakt van een 5×5 rooster, waarin de letters van het alfabet in een willekeurige volgorde uitgeschreven worden. Omdat ons alfabet 26 letters telt, worden de letters I en J als één letter gezien. Eerst worden de letters van een bepaald sleutelwoord in het rooster ingevuld, van links naar rechts en van boven naar onder. Daarbij worden herhaalde letters in het sleutelwoord weggelaten. Daarna worden de overige posities in het rooster van links naar rechts en van boven naar onder ingevuld met de ontbrekende letters van het alfabet, in volgorde waarin de letters in het alfabet voorkomen. Als we deze procedure toepassen met het sleutelwoord STALINGRAD, dan wordt bijvoorbeeld de tweede A overgeslagen, en worden de letters op de volgende manier gerangschikt in het rooster.

S T A L I/J
N G R D B
C E F H K
M O P Q U
V W X Y Z

Om een bericht te versleutelen, wordt de tekst eerst opgedeeld in bigrammen (groepen van twee letters). Karakters in de tekst die geen letter zijn (leestekens, spaties, …) worden hierbij genegeerd. Indien een bigram uit twee identieke letters zou bestaan, dan wordt daartussen een X (of een Q indien de letters zelf een X zijn) toegevoegd in de tekst. Indien er op het einde slechts één letter overblijft, dan wordt die in het laatste bigram aangevuld met een X (of een Q indien de laatste letter zelf een X is). De tekst Dit is een zeer geheim bericht. wordt bijvoorbeeld als volgt opgedeeld in bigrammen:

DI TI SE EN ZE ER GE HE IM BE RI CH TX

Daarna wordt elk bigram omgezet naar een gecodeerd bigram op basis van de volgende regels:

- Als de letters in het rooster op dezelfde rij staan, dan vervangen we elke letter door zijn rechterbuur in het rooster. De rechterbuur van een letter in de laatste kolom van het rooster is de letter in de eerste kolom op dezelfde rij.
- Als de letters in het rooster op dezelfde kolom staan, dan vervangen we elke letter door zijn onderbuur in het rooster. De onderbuur van een letter in de onderste rij van het rooster is de letter in de bovenste rij op dezelfde kolom.
- Als de letters in het rooster niet op dezelfde rij of kolom staan, dan vervangen we elke letter door de letter die op dezelfde rij staat en een ander hoekpunt is van de rechthoek die gevormd wordt door de letters in het oorspronkelijke bigram. Hierbij is de volgorde belangrijk — de eerste letter van het gecodeerde bigram is de letter die op dezelfde **rij** staat als de eerste letter in het oorspronkelijke bigram.

Het eerste bigram DI van de voorbeeldtekst vormt een rechthoek in het rooster, waarvan de andere hoekpunten de letters B en L zijn (met B op dezelfde rij als D en L op dezelfde rij als I).

```
. . . L I/J
. . . D B
. . . . .
. . . . .
. . . . .
```

Na codering van het eerste bigram krijgen we dus

```
DI TI SE EN ZE ER GE HE IM BE RI CH TX
BL
```

Bij het volgende bigram TI vinden we beide letters in dezelfde rij van het rooster. We nemen dan de letters onmiddellijk rechts ervan op diezelfde rij. Omdat de letter I uiterst rechts staat op de eerste rij, wordt die vervangen door de letter S uiterst links op de eerste rij.

```
S T A . I/J
. . . . .
. . . . .
. . . . .
. . . . .
```

Het bigram TI wordt op die manier dus gecodeerd als het bigram AS. De volgende vier bigrammen worden telkens gecodeerd op basis van de derde regel, omdat de letters nooit op dezelfde rij of kolom staan. We hebben dus voorlopig de volgende versleuteling gevonden.

```
DI TI SE EN ZE ER GE HE IM BE RI CH TX
BL AS TC CG WK FG
```

Bij het bigram GE vinden we beide letters in dezelfde kolom van het rooster. We nemen dan de letters onmiddellijk eronder op diezelfde rij, waardoor het bigram wordt gecodeerd als het bigram EO.

```
. . . . .
. G . . .
. E . . .
. O . . .
. . . . .
```

Alle mogelijke situaties zijn nu geïllustreerd en we kunnen de overige bigrammen als volgt

coderen.

DI TI SE EN ZE ER GE HE IM BE RI CH TX
BL AS TC CG WK FG EO KF SU GK BA EK AW

Om een gecodeerd bericht te ontcijferen moeten we enkel het proces omkeren. Voor rechthoeken kiezen we opnieuw de tegenoverliggende hoeken, voor letters in dezelfde rij kiezen we de letters onmiddellijk links ervan, en voor letters in dezelfde kolom kiezen we de letters onmiddellijk erboven.

Opgave

Definieer een klasse Playfair waarmee teksten kunnen gecodeerd en gedecodeerd worden volgens Playfair met een gegeven sleutelwoord. Bij het coderen en decoderen mag nooit onderscheid gemaakt worden tussen hoofdletters en kleine letters, en tussen de letters I en J. In gecodeerde en gedecodeerde berichten moeten alle letters uitgeschreven worden als hoofdletters, en wordt de letter I/J genoteerd als de letter I. Deze klasse moet ondersteuning bieden aan de volgende methoden:

- Een initialisatiemethode waaraan een sleutelwoord moet doorgegeven worden. Dit is het sleutelwoord waarmee het rooster opgebouwd wordt voor het coderen en decoderen van bigrammen.
- Een methode bigram waaraan een string moet doorgegeven worden. Indien deze string geen bigram met twee verschillende letters is, dan moet de methode een AssertionError opwerpen met de boodschap geen twee verschillende letters. De methode heeft ook nog een optionele parameter codeer waaraan een Booleaanse waarde kan doorgegeven worden (standaardwaarde: True) . Indien de waarde True wordt doorgegeven aan de parameter codeer, dan moet de methode het gecodeerde bigram teruggeven voor het gegeven bigram. Indien de waarde False wordt doorgegeven aan de parameter codeer, dan moet de methode het gedecodeerde bigram teruggeven voor het gegeven gecodeerde bigram.
- Een methode codeer waaraan een string moet doorgegeven worden. De methode moet de gecodeerde string teruggeven na codering van de gegeven string door Playfair met het opgegeven sleutelwoord.
- Een methode decodeer waaraan een string moet doorgegeven worden. De methode moet de gedecodeerde string teruggeven na decodering van de gegeven string door Playfair met het opgegeven sleutelwoord. Indien er tijdens het coderen van de gegeven string extra letters X of Q werden toegevoegd aan het oorspronkelijke bericht, dan moet de methode die niet uit het gedecodeerde bericht verwijderen.

Bovendien moet het mogelijk zijn om met de ingebouwde functie print een stringvoorstelling uit te schrijven van elk object van de klasse Playfair. Deze stringvoorstelling vormt een weergave van het rooster dat gebruikt wordt bij de codering/decodering, in het formaat zoals aangegeven in onderstaand voorbeeld.

Voorbeeld

```
>>> play = Playfair('STALINGRAD')
>>> print(play)
STALI
NGRDB
CEFHK
```

```
MOPQU
VWXYZ
>>> play.bigram('DI')
'BL'
>>> play.bigram('ti')
'AS'
>>> play.bigram('Ge')
'EO'
>>> play.bigram('BL', codeer=False)
'DI'
>>> play.bigram('as', codeer=False)
'TI'
>>> play.bigram('Eo', False)
'GE'
>>> play.bigram('A')
Traceback (most recent call last):
AssertionError: geen twee verschillende letters
>>> play.bigram('AA')
Traceback (most recent call last):
AssertionError: geen twee verschillende letters
>>> play.bigram('ABC')
Traceback (most recent call last):
AssertionError: geen twee verschillende letters
>>> play.codeer('Dit is een zeer geheim bericht.')
'BLASTCCGWKFGEOKFSUGKBAEKAW'
>>> play.decodeer('BLASTCCGWKFGEOKFSUGKBAEKAW')
'DITISEENZEERGEHEIMBERICHTX'
```

Bronnen

- **Mauborgne JO (1914).** An Advanced Problem in Cryptography and Its Solution. *Army Service Schools Press*.
- **Gaines HF (1956).** Cryptanalysis: a study of ciphers and their solutions. *DOVER*.
- **Smith M (1998).** Station X: The Codebreakers of Bletcheley Park. *Channel 4 Books/Macmillan, London*.