ESIEE Paris
IGI-3008

Cryptographie

Léa MENERET, Fathima SAHADATTALY, Ulrike KULZER

4. November 2017

1 Contexte

1.1 En général

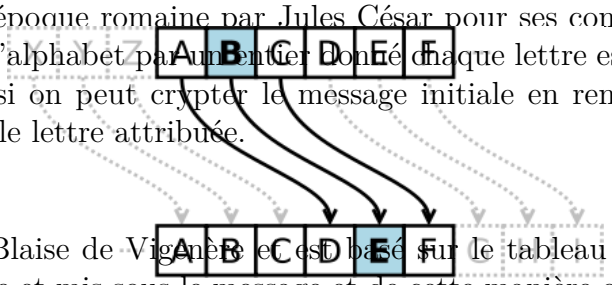
La cryptographie est une technique utilisée pour rendre incompréhensible à autrui un message entre un expéditeur et un destinataire. Ce procédé a notamment été utilisé en période de guerre pour permettre des attaques surprises. Le principe est le suivant : L'expéditeur à partir d'une clé crypte son message et l'envoie au destinataire. Celui-ci possède aussi la clé qui va lui permettre ainsi de décrypter le message.

1.2 Histoire

La cryptographie est utilisée depuis l'Antiquité mais certaines de ces méthodes les plus abouties datent du 20e siècle. Il existe différents principes de cryptage plus ou moins compliqués tels que

- *le chiffre de César :*

  Ce procédé a été inventé lors de l'époque romaine par Jules César pour ses communications secrètes. En décalant l'alphabet par un entier donné chaque lettre est associée à une nouvelle lettre, ainsi on peut crypter le message initiale en remplaçant chaque lettre par la nouvelle lettre attribuée.



- *le chiffre de Vigenère :*

  Il a été inventé au 16e siècle par Blaise de Vigenère et est basé sur le tableau à droite. Une clé (un mot) est répétée et mis sous le message et de cette manière on peut trouver les lettres correspondantes à partir du tableau.

  Exemple: Clé : musique
  Texte : J'adore écouter la radio toute la journée.
  Texte en claire : j'adore ecouter la radio toute la journee
  Clé répétée : M USIQU EMUSIQU EM USIQU EMUSI QU EMUSIQU
  ~~~~

  | ||Colonne O, ligne I : on obtient la lettre W.
  | |Colonne D, ligne S : on obtient la lettre V.
  | Colonne A, ligne U : on obtient la lettre U.
  Colonne J, ligne M : on obtient la lettre V.
  ~~~~

2 Fonctionnalité

2.1 En général

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

2.2 En détail et coupé en modules

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

3 Interfaces utilisateurs

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

3.0.1 Das Farbmodell HSV

3.0.2 Die Farbmodelle YUV, YPbPr und YCbCr

$$hue := \begin{cases} 0.0, & \text{for } max\_value = min\_value \\ 60.0 \cdot \left(0.0 + \frac{g-b}{max\_value-min\_value}\right), & \text{for } max\_value = r \\ 60.0 \cdot \left(2.0 + \frac{b-r}{max\_value-min\_value}\right), & \text{for } max\_value = g \\ 60.0 \cdot \left(4.0 + \frac{r-g}{max\_value-min\_value}\right), & \text{for } max\_value = b \end{cases}$$

$$satVal := \begin{cases} 0.0, & \text{for } max\_value = 0.0 \\ \frac{max\_value-min\_value}{max\_value}), & \text{otherwise} \end{cases}$$

Abb. 4: Originalbild

Abb. 5: Bild nach der Konvertierung

Abb. 6: Bild im HSV-Farbraum

Abb. 7: Bild nach der Konvertierung

Abb. 8: RGB nach HSV
Quelle: w.hsv

Abb. 9: HSV nach RGB mit vergrößertem Ausschnitt

4 Referenzen

Bildquellen

Abb. ?? http://www.itwissen.info/definition/lexikon/Standard-RGB-sRGB-standard-RGB.html (31.01.2017)

Abb. ?? https://www.saxoprint.de/blog/der-farbraum-rgb-und-cmyk-im-vergleich/ (31.01.2017)

Abb. ?? http://de.mathworks.com/help/images/convert-from-hsv-to-rgb-color-space.html?requestedDomain=www.mathworks.com (07.02.2017)

Abb. 4 Ulrike Kulzer

Abb. 8 Originalbild: https://www.tutorialspoint.com/java_dip/color_space_conversion.htm (08.02.2017)

Naher Osten 65%
Lateinamerika 13%