**Le cryptage R.S.A**

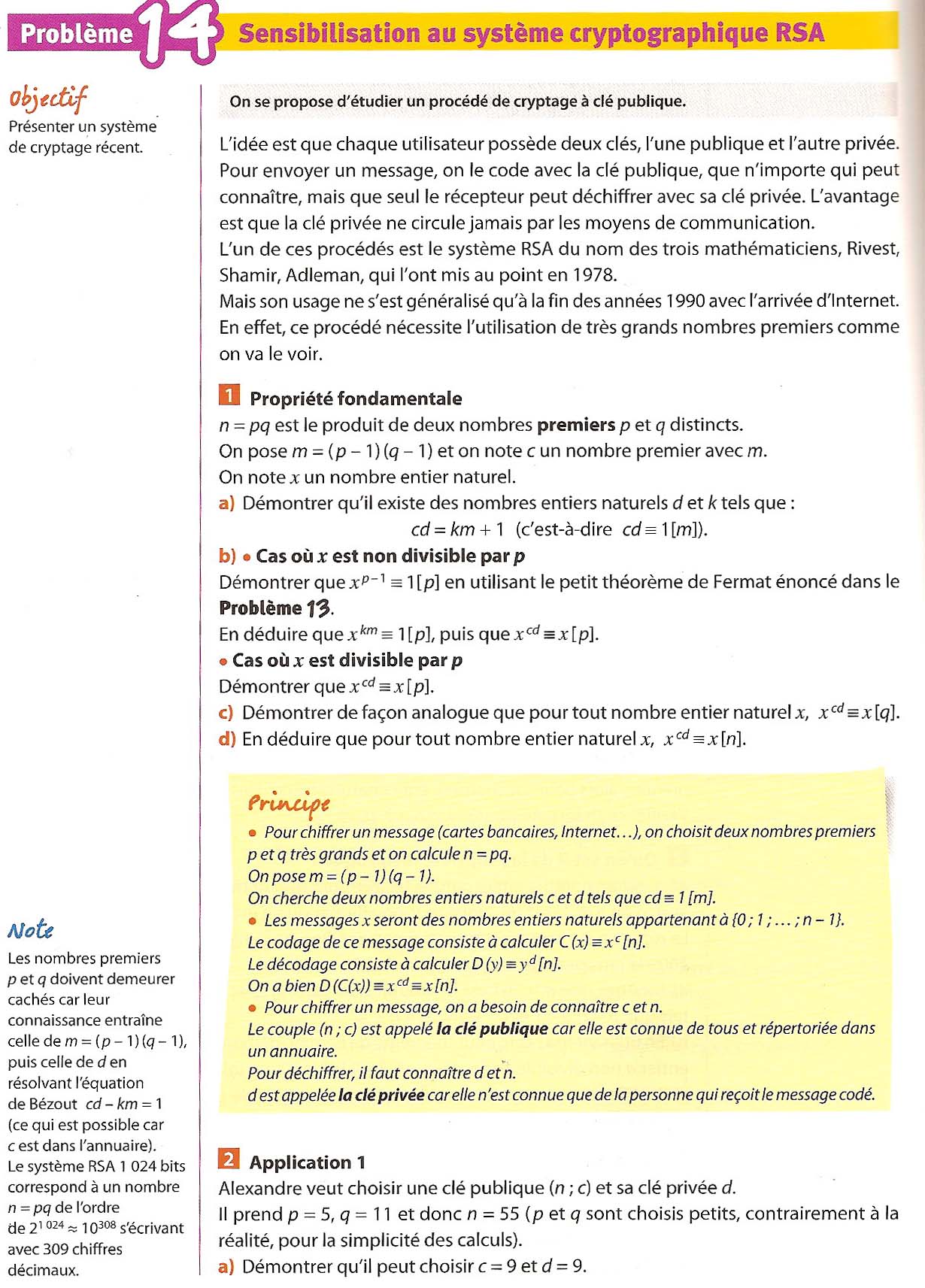
1. **Résumé de la méthode**

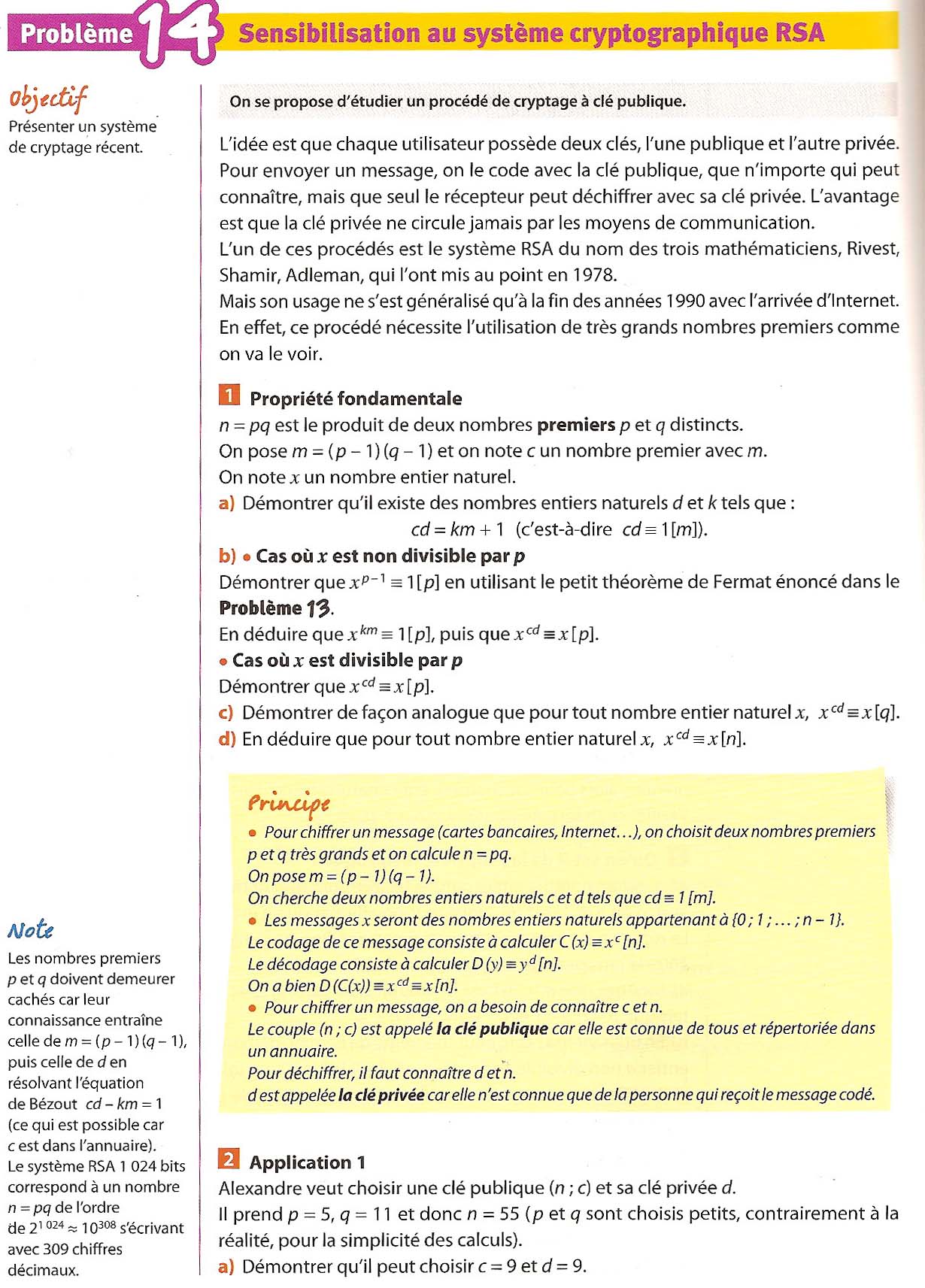
* Chaque lettre de l’alphabet est numérotée, dans l’ordre, de 1 à 26
* Soient deux nombres premiers p et q, qui restent secrets, on pose n = pq > 26 et m = (p – 1)(q – 1)
* Soit c un nombre premier avec m : **le couple (c,n) est la clef publique**, elle est connue de tous
* Soit d un nombre entier, qu’il est possible de **choisir tel que cd 1 [m]** : **d est la clef privée**, connue uniquement de la personne qui reçoit le message.
* ***Principe du cryptage :***
  + Si *x* est le numéro d’une lettre, **son cryptage c(*x*) est le reste de la division de *x*c par n (c'est-à-dire que xc c(x) [n])**
* ***Principe du décryptage :***
  + **Théorème : pour tout *x* , *x*cd *x* [n]**
  + **donc, si y est un chiffre crypté, son décryptage d(y) est le reste de la division de yd par n**

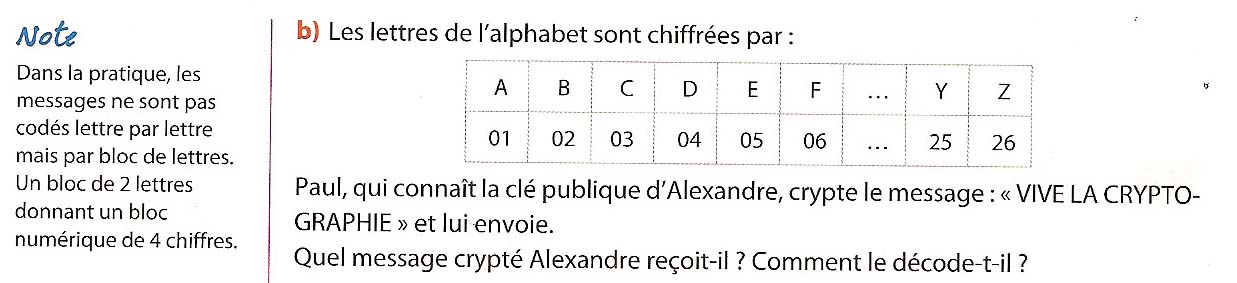
*yd = (xc)d = xcd x [n]*

1. **Présentation avec les outils de terminale S – spé maths (chapitre des nombres premiers)**

Tiré du livre *Hyperbole programme 2012*







***Correction de l’application :***

* p et q sont deux nombres premiers, et n = 511 = 55
* m = 410 = 40 : on peut choisir c = d = 9 car 99 = 81, qui est congru à 1 modulo 40
* Je crypte « VIVE » (c'est-à-dire 22 – 9 – 22 – 5) avec la clef publique (9,55)
  + 229 22 [55] , 99 49 [55] , 59 20 [55]
  + Ainsi, le mot VIVE est codé par 22 – 49 – 22 – 20
* Pour décrypter, même opération avec d = 9

1. **Schéma – Bilan :**

*c(x) = reste division de xc par n*

*x*

*Clef publique (n, c)*

CRYPTAGE

**MESSAGE CLAIR MESSAGE CRYPTE**

DECRYPTAGE

****

*x = reste division de c(x)d par n*

*c(x)*

*Clef privée (n,d)*

1. **Présentation avec les outils de l’enseignement supérieur (anneau /n)**

* **Définition :** Soit n un entier, n>1. On appelle ***indicateur d’Euler*** (n) le nombre d’entiers qui sont premiers avec n. Il est équivalent de dire que (n) est le nombre d’éléments inversibles de /n
* **Quelques propriétés :**

Soit n un entier, n>1

**(1) Si k est un entier premier avec n, alors k(n) 1 [n]**

Cette propriété constitue une généralisation du théorème de Fermat (si pgcd(k,n) = 1 alors kn – 1 1 [n])

**(2) Si l’on considère la décomposition en facteur premiers de alors :**

**(n) = n**

**En particulier si n = pq alors (n)=(p – 1)(q – 1)** ce qui est utile dans notre application

Et enfin le **théorème du cryptage**

**(3) Soient p et q deux nombres premiers distincts, et n = pq.** (donc(n)=(p – 1)(q – 1) )

**Si c et d sont deux entiers tels que cd 1 [(n)] alors, pour tout t , tcd t [n]**

Dans **/n**, l’application est la ***fonction de chiffrement***

Dans **/n**, l’application est la ***fonction de déchiffrement***

Ces deux applications sont réciproques d’après le théorème (3) d’où le résultat.

1. **Démonstration du théorème (3) avec les outils de l’enseignement supérieur**

La démonstration du ***théorème 1*** est immédiate (si pgcd (k,n) = 1 alors est inversible dans /n…).

La démonstration du ***théorème 2*** est plus complexe, elle repose sur le « lemme des chinois » : si p et q sont deux entiers premiers entre eux, alors les anneaux /p et /q sont isomorphes à l’anneau /pq

La démonstration du ***théorème 3*** repose sur le théorème de Fermat, le théorème (2) et le théorème de Gauss (ce dernier vu en term S) :

Le choix de p et q fait que (n)=(p – 1)(q – 1)

Soit alors un entier k vérifiant : cd = 1 + k(n), on a alors cd = 1 + k(p – 1)(q – 1) ; et soit t

* *Premier cas : pgcd(t,p) = 1*, on a donc tp – 1 1 [p] d’après le théorème de Fermat

Donc =

* *Deuxième cas : pgcd(t,p) 1*, on a alors p|t donc tcd 0 t [p]

De même, tcd 1 [q]

Ainsi, p|tcd – t donc tcd – t peut s’écrire sous la forme p, entier

q|tcd – t donc q|p donc q| par application du théorème de Gauss (p et q sont premiers entre eux), et donc tcd – t peut s’écrire sous la forme pq, entier

d’où pq| tcd – t

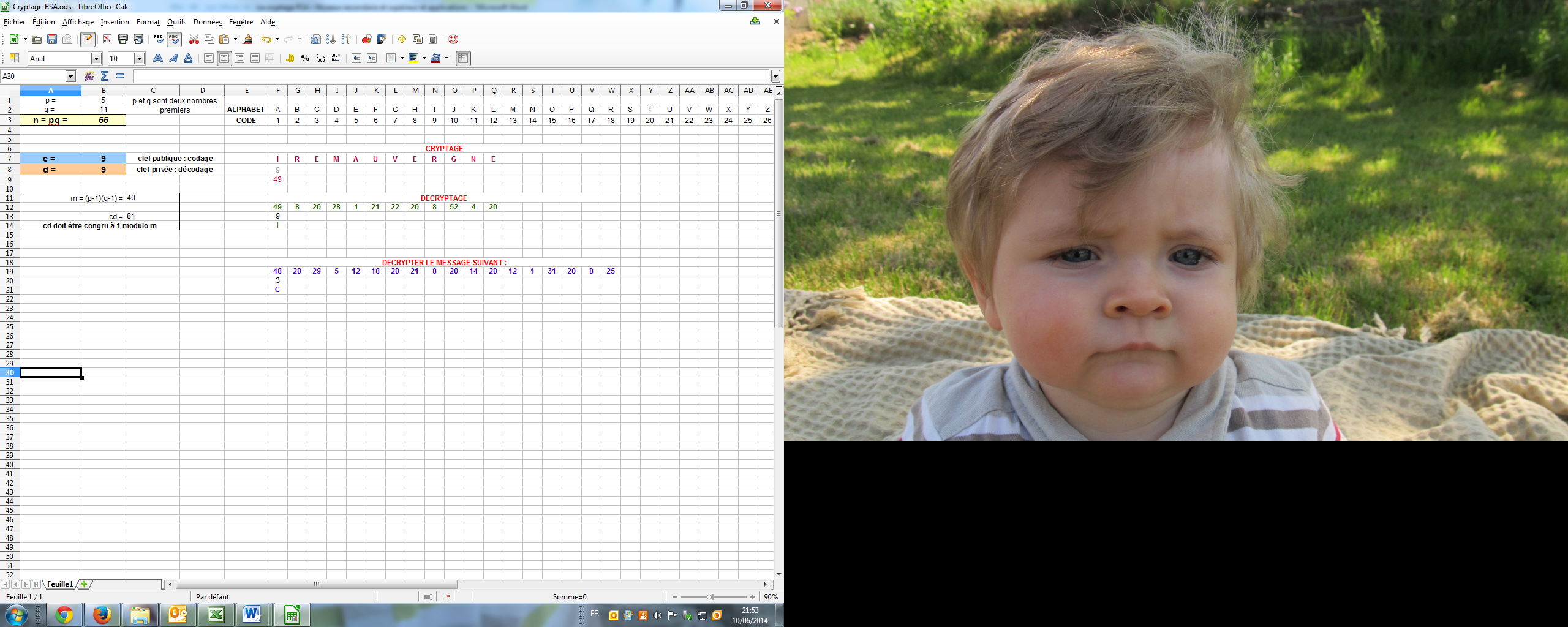
donc tcd t [n] (rappelons que n = pq)

1. **Application : programmation avec le logiciel LibreOffice**

***Nom du fichier :*** Cryptage RSA.ods

***Fonctions utilisées :***

* **MOD :** MOD(a ;b) renvoie le reste de la division euclidienne de ab par b
* **RECHERCHE :** recherche le rang d’une valeur donnée dans un vecteur (ordonné) origine, puis renvoie la valeur inscrite au même rang dans un vecteur résultat



* En F8  =RECHERCHE(F7;$F$2:$AE$2;$F$3:$AE$3)
* En F9 =MOD(F8^$B$7;$B$3)
* En F13 =MOD(F12^$B$8;$B$3)
* En F14 =RECHERCHE(F13;$F$3:$AE$3;$F$2:$AE$2)
* En F20 =MOD(F19^$B$8;$B$3)
* En F21 =RECHERCHE(F20;$F$3:$AE$3;$F$2:$AE$2)

Utilisation de références absolues (siglées $) impératives afin de recopier les formules et former des mots.