Université Paris Est Créteil Val de Marne Licences d'Informatique 2013-2014

## Mathématiques discrètes pour l'informatique

Contrôle continu 2, le 20 mars 2014. Durée 30 minutes. (Sans documents. Les calculatrices sont autorisées.)

[3pts] Question 1 : Congruences

Résoudre le système de congruences suivant

$$(S_2) \begin{cases} x \equiv 5 \pmod{123} \\ x \equiv 5 \pmod{20} \end{cases}$$

[7pts] Question 2: RSA

NOM et PRENOM:

On considère le système cryptographique RSA avec la clé publique (n, e) = (77, 53).

- 1. Le couple (n, e) est-il une clé publique possible pour RSA? Justifiez.
- 2. Quelle est la clé secrète  $(\varphi(n), d)$  qui permet de décoder les messages?
- 3. Quel est le cryptogramme du message M=25?
