Enoncé TP

Vous travaillez en tant qu'espion pour une agence gouvernementale et devez à tout prix décoder le message contenant des informations précieuses à la capture d'un criminel.

Tout ce que vous savez est que le message est codé avec l'algorithme RSA et vous avez intercepté les éléments publics du message, à savoir :

La clé publique suivante :

$$n = 1190836873$$
$$e = 1051$$

Votre intuition vous dit que les deux premiers utilisés pour générer la clé publique ont le même ordre de grandeur et que le message utilise l'encodage UTF-8 standard (8 bits par charactère).

Le message intercepté est composé de divers paquets comme suit (les blocs sont ordonnés par colonne) :

---Coded message-	367266109	259270170	272927971
139625027	273461422	120667892	584586872
728808256	593918599	994450868	462362840
677396451	807072360	456798524	643206446
662265473	1029159804	411559218	54682859
845995352	243815344	1033648476	691867698
613303937	710536598	600727524	704691074
1033970589	219532422	40042580	1010665647
623160996	339194689	247503992	426396134
1160483016	1115370236	913555530	775579937
243815344	803893657	483175114	6952392
572050792	806790933	22363795	-----End message ----
495107014	145790893	805184996	
909878795	601459052	581234996	

Faites un rapport décrivant comment vous avez déchiffré le message.

Faites également une analyse de la performance de votre approche, et estimez le temps qu'il vous faudrait pour déchiffrer une clé ayant non pas 10 chiffres, mais 200 !!!

Rapport et rendu

1. Pensez à donner le nom complet de chaque membre du groupe en première page,

2. Ecrivez une brève introduction sur le contexte du TP. Soyez créatifs pour mentionner les fondements théoriques du cours sans pour autant copier les slides !

3. Décrivez COMMENT vous avez implémenté les méthodes – sans pour autant fournir votre code ni une documentation de ce dernier.
   Le but est de décrire les astuces d'implémentation non triviales. Donnez au moins le nom des méthodes implémentées (dans la théorie, pas dans le code !), ainsi que les astuces d'implémentation (exemple typique : le pgcd assume que le premier nombre est le plus grand…).

4. Présentez vos résultats ainsi qu'une analyse de la performance (basée sur des mesures et/ou des approximations pour les très grands nombres, comme vu au cours).

5. Pensez à TOUJOURS justifier vos propos. Evitez les « on sait que », « on montre que » ou les conclusions non-justifiées du type « A est plus complexe que B ». Posez-vous toujours la question « pourquoi est-ce le cas » et, si la réponse n'est pas triviale, expliquez (parfois, 3 mots suffisent !).

6. Pour la structure, il vous faudrait une introduction, une motivation théorique, une partie méthodologique, la présentation des résultats ainsi qu'une conclusion.

7. Le rendu du tp se fait sous forme électronique : le rapport sous forme PDF, le code-source sous forme d'archive (.zip ou autre).