

Cryptography Assignment 2

Like many of your fellow students, you have started a lucrative consulting business using the expertise you gained in **Cryptography** to work on the international cryptography scene. You quickly built a large clientele, and learned to recognise the naïve cryptographic implementations of your clients' competitors (who did not successfully complete the AMSI **Cryptgraphy** at Sydney Uni).

1. (*LFSR Stream Cipher*). You intercept two outgoing ciphertext messages from your adversary, which you believe have the same content, enciphered for different parties. You have reason to believe that Bond's agency is using a simple stream cipher generated by a LFSR, with unbuffered ASCII encoding the message text. Previous messages have always begun with the header:

To: James S. Bond <007@hmss.gov.uk>

The message is supposed to notify agent 007 of a change of meeting place from the *Friend in Hand* in Glebe to a new location. Having already made elaborate plans for a special surprise party at the *Friend in Hand*, your client would like to have the meeting take place as originally arranged. Decipher the message, change its contents to confirm the meeting, and re-encipher each message using its original cipher.

2. (*El Gamal Cryptosystem*). At a special party for your most trusted client you mentioned that their competitors never test whether $p - 1$ is smooth¹ for the primes p used in El Gamal cryptosystems. Having celebrated a bit too much with champagne, you boasted that you could break the cipher whenever $p - 1$ has no prime factors larger than 10 digits. Weeks later, and long after you forgot about this boast, your client returns to you with a ciphertext sample, sorted from among thousands of intercepted messages. Return the plaintext and the private key to the client.

3. (*RSA Cryptosystem with Small Exponent*). One of your clients presents you with an RSA ciphertext sample enciphered with public exponent $e = 3$. You know it is hopeless to decipher from this information, but the client mentions that there was a flurry of messages sent out simultaneously on that particular day. From your work in the field, you know that the competitor doesn't buffer the plaintext, and that this particular organization is watched by several clients of your former **Cryptography** classmates. Use whatever means necessary to recover the plaintext.

Answers to the assignment should be submitted by Thursday 8 February 2007.

¹Having picked up the term *smooth* — the property of having only small prime factors — from your number theory friends, you felt like throwing out some new terminology to impress your clients