MATH 3024 Assignment 02

Like many of your fellow students, you have started a lucrative consulting business using the expertise you gained in MATH3024 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 MATH3024 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 smooth[1] 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 MATH3024 classmates. Use whatever means necessary to recover the plaintext.

4. *(Shamir Secret Sharing).* You are consulting for an organization which would like to obtain the secret key distributed among several individuals by the Shamir perfect secret sharing scheme. In one of your most lucrative rates, in a twenty minute session you collected \$1,000 for informing the client that it would be theoretically impossible to break a Shamir $(3, 6)$-threshold secret sharing scheme with only two keys. Three days later, to your surprise, the client returns with three keys. Solve for the secret key.

[1] Having 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

5. *(RSA Signature Scheme).* Generate a unique RSA public-private key pair for an RSA modulus of up to 192 bits. Provide your RSA public key as a response to this question and the following declaration:

`$LOGIN, $DD.MM.YYYY.`

where `$LOGIN` is your departmental login and `$DD.MM.YYYY` is the submission date. Append the bit-encoded RSA signature of this declaration to your assignment. Hint: verify the signature with your public key.

Answers to the assignment should be submitted by Thursday 10 June 2004. Consult the course web page for submission details.