P.Lafourcade, G.Marcadet

Session 2

Exercise 1 (Scytale)
David has intercepted the following message:

SUTSTRUISREERYNAOCTAOSCIIOPDTIPCS

Knowing that it has been generated using a scytale, what is the message that he will read?

Exercise 2 (Polybius Square)
The Polybius square, also known as the Polybius checkerboard, is a device invented by the Ancient Greek historian and scholar Polybius, for fractionating plaintext characters so that they can be represented by a smaller set of symbols.

1. Use the hint to decrypt the following ciphertext:
   21 34 42 44 54-44 52 34: 44 23 15 11 33 43 52 15 42 44 34 31 24 21 15
2. Can you deduce how the Polybius square works?

Hint: Jim Moriarty
23 24 33 44: 24 24 32 32 34 42 24 11 42 44 54

Exercise 3 (RSA encryption)
1. Recall how to encrypt and decrypt with the RSA cryptosystem.
2. Let $p = 3$, $q = 11$, compute n and $\Phi(n)$.
3. Let $e = 7$, encrypt the plaintext $M = 2$.
4. Compute the associated d and decrypt the ciphertext $C = 3$.
5. Recall the prime factorization problem.
6. Find and prove the homomorphic property of RSA cryptosystem.

Exercise 4 (ElGamal Encryption)
1. Recall the ElGamal encryption.
2. Let $a = 2$ and $(p, g) = (5, 3)$, compute h and decrypt the ciphertext $C = (4, 2)$.
3. Check that the message found in the previous question gives C if $r = 2$ is used.
4. Recall the discret logarithm problem.
5. Find and prove the homomorphic property of ElGamal cryptosystem.

Exercise 5 (RSA attacks)

1. (a) Recall the homomorphic property of RSA. Use this fact to find an expression of $\text{Dec}(c_1 \times c_2)$ where Dec is the decryption function, and c_1 and c_2 the ciphertexts of m_1 and m_2, respectively.

   (b) You are given a ciphertext c that you must decrypt. You are given an encryption oracle (letting you encrypt any message), and a decryption oracle (letting you decrypt any message, except c). How do you retrieve the cleartext of c?

2. Alice has an RSA keypair, which public key is $N_1 = pq$. She wants to generate another keypair, for other purposes. In order to save time and trying to be clever, she only generates another prime r, and uses $N_2 = qr$. Describe how to break both keys in a matter of microseconds.

Note: questions 1 is one of the reasons why "classic" RSA is never used in real life (instead, we use RSA PKCS#1 v1.5 or even better, RSA PKCS#1 OAEP, or other encryption systems) Question 2 can be summed up as "never try to be clever when using crypto, and never code your own crypto".

Exercise 6 (Zheng and Seberry)

Zheng and Seberry in 1993 propose the following encryption scheme:

$$f(r)||(G(r) \oplus (x||H(x))) \ ,$$

where x is the original message, f is an one-way function with trap (like RSA), G and H are two public hash functions, $||$ denotes the concatenation of strings and $\oplus$ is the XOR operation. Give the associated decryption algorithm.

Exercise 7 (ElGamal with Elliptic Curves)

We consider the ElGamal cryptosystem with elliptic curves. Let E be an elliptic curve over a field $\mathbb{F}_q$ (with q a prime number) and a point P of order N.

1. Give a secret key and the associated public key.

2. How to encrypt a message $M \in E$ using ElGamal cryptosystem using the elliptic curve E?

3. How to decrypt the ElGamal ciphertext $(C_1, C_2) \in E^2$?