Computer Security – Tutorial Sheet 1
Cryptography

School of Informatics
University of Edinburgh

23rd January 2014

This is the first question sheet for the Computer Security course, covering topics in cryptography. Tutorial question sheets are provided to help guide your self-study on the course and measure your progress. The process for this tutorial sheet is as follows:

1. Read and try to answer these questions before your Week 3 tutorial.
2. The tutor will discuss answers to *some* questions at the Week 3 tutorial.
3. After the Week 3 tutorial, write down your answers to all questions.
4. In Week 5, a solution sheet will be issued. To measure your understanding of the material, use the solution sheet to assess your own answers.
5. In the final tutorial, there will be an opportunity to raise problem points in any of the tutorial questions with your tutor.

You are encouraged to discuss this tutorial with other students and work together to ensure that you fully understand the concepts covered. This does *not* apply to questions on the assessed practical exercises, issued separately.

Part A: RSA

1. To familiarise yourself with the RSA algorithm, prove its correctness. Recall that the modulus n is the product of two large random secret primes, e is a random integer that forms the public key (together with n). Now show that decryption is the inverse of encryption: if $c = m^e \bmod n$, then $c^d \bmod n = m$.

2. Suppose you were given the following:

$$\begin{aligned} n &= 26085133416023792110786950746751186556 9 \\ d &= 11419990338673736177884281093720685329 1 \\ c &= 25659792217239235040146736902131445688 5 \end{aligned}$$

   What is the message?
   (**Hint**: In python use the gmpy package, available on student.compute, to perform efficient calculations with large numbers. In IPython, type `import gmpy` then `help(gmpy)`.)

3. Now suppose you were given the following:

$$\phi(n) = 26085133416023792107536546297113106144 4$$

   What are p, q and e?
   (**Hint**: can you write a quadratic equation with p and q as the roots?)

Part B: Vigenère cipher

The *Vigenère toy cipher* is a polyalphabetic substitution cipher with a block size of 3, that operates on octal digits $\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and uses three alphabet rearrangements, rotating each letter of the alphabet to the right by 2, 3, and 5 positions, respectively.

1. Encode the plaintext `123452034521` using the Vigenère cipher.
2. What is the main reason that the Vigenère cipher is only a toy, and how would you cryptanalyse this cipher?
3. How can the polyalphabetic substitution cipher be improved to make an unbreakable cipher, and what's the disadvantage of this method?

Part C: DLP and ElGamal

The *discrete logarithm problem* (DLP) is the problem of finding the smallest positive integer x which is a solution to the modular exponentiation equation:

$$\beta \equiv \alpha^x \bmod n$$

for a given α, β, n, where α is usually a generator and β any element of the multiplicative group $Z^\star[n] = \{1 \leq a < n \mid \gcd(a, n) = 1\}$. Solving the DLP in general is considered to be infeasible for large n.

1. Show $Z^\star[10]$ and by tabulating the powers of its elements, find which elements are generators.
2. The ElGamal algorithm for encryption is also believed to rely on the difficulty of the DLP. Here is a reminder of the construction. If Alice wants to send a message to Bob, she first obtains his public key (p, α, β), where p is a large prime. Then she generates a random number r and encrypts her message m into a pair:

$$E(m) = (g, d) \qquad \text{where} \quad \begin{aligned} g &= \alpha^r \bmod p \\ d &= m\beta^r \bmod p. \end{aligned}$$

   Using his (randomly chosen) private key k, Bob can decrypt this by:

$$D(g, d) = dg^{-k} \bmod p$$

   which works because $dg^{-k} \equiv m\beta^r \alpha^{-rk} \equiv m \pmod p$ and $\beta = \alpha^k \bmod p$ (note: it is feasible to compute inverses like g^{-k}).

   (a) Compared with RSA, name the immediately apparent disadvantage of the ElGamal encryption function.

   (b) Considering the role of random numbers, explain informally why an eavesdropper cannot decrypt the pair (g, d).

   (c) It is essential that Alice chooses a fresh random number r for each message she encrypts. Explain what can go wrong if this does not happen (**Hint**: consider a known plaintext).

3. In the equation above, what would happen if we allowed α to be a non-generator, and what might the impact of this be on its use in an encryption algorithm such as ElGamal?

Part D: Security Situations

The following situations require information to be transfered over insecure channels. Describe and discuss any security issues that arise (e.g., how easy it is to eavesdrop and break confidentiality). Give a recommendation in each case that you consider would be adequate.

1. You would like to securely forward a terminal from your Raspberry Pi to another computer.
2. You would like to buy something online, this will require you sending your bank card details over the internet.
3. James Bond has been chasing bad guys around Europe, he needs to securely transfer some very sensitive information back to MI6 headquarters.
4. You are away on holiday and your parents (who aren't very technologically inclined) want to know the password for the router.
5. Obama wants to call Putin to talk about something top secret.

Questions by Luke Shrimpton and David Aspinall.
Issued by Daniel Franzen, DA and MA.