# Crypto SD Revision Question and Answers

### *Is the exam going to be multiple choice or essay?*

The exam will involve problem solving and essays type questions.

There will NOT be any multiple choice questions.

You will have to answer all questions.

### *Are the exams based on the lecture slides only?*

The exams are based on the material presented during the course, which includes lecture slides, recorded lectures and interactive lectures.

### *Are Past Papers Helpful?*

Last year's paper is most helpful because it was answered remotely, just like this year.

The papers from years before then are a bit helpful, but remember that they were designed for students answering them in a traditional exam hall. Discount questions that can be answered just by looking up the course materials since they would be too easy under this year's exam conditions.



### *Euler's Theorem : Why must gcd(P,n) = 1?*

Proof that decryption undoes encryption relies on $P^{\Phi(n)} \% n = 1$. This is a version of Euler's theorem, which is only true if gcd(P,n) = 1. This is just a property of the underlying mathematics. If it is not true then encryption followed by decryption will produce a different number than the one we started with. P is the plain text.

### *RSA : How are Prime Numbers p and q chosen?*

The length of n (the number of bits) is chosen based on international standards.

Each prime has half the number of bits.

A random number with this number of bits – 2 is chosen with a secure random number generator. The bits 11 are added in the least significant bit positions. This generates an odd number where p % 4 = 3.

This number is tested to see if it is a prime. If not, then 4 is added and the test repeated until a prime is found.

This process is repeated for the second prime.

### *Caesar Cipher Rotor Machine*

**(b)** Give an example of a 4 rotor machine where each rotor implements a Caesar cipher with shifts 3, 15, 7, 4. The alphabet consists of the 26 English letters plus space, comma, fullstop. Show how your machine both encrypts and decrypts?

[6]

This is not an Enigma machine. This is an open ended question to test your understanding of rotor machines. Half marks are earned by a general description of how rotor machines work. More marks are obtained by also noticing that a Caesar

cipher is not very good for a rotor machine because the substitution is always the same no matter what position the rotor is in. The final mark is obtained by noticing that 3+15+7+4 = 29, the number of letters on the rotor. So the cipher text is always the same as the plain text.

### *What does R=4.7 in English Mean?*

There are 26 letters in the English alphabet. If each is equally likely to occur then the entropy formula gives $\log_2(26) = 4.7$.

### *How is r Calculated?*

r is the entropy per letter based on actual frequencies of letters in the English language. It is found experimentally and depends on the size of text segment, ie N. If N = 1 it is just the single letter frequency, if N = 2 it the frequency of all letter pairs, and so on. Spaces are not normally included. As N increases, the value of $r_N/N$ tends to the same value, which is the overall value of r.

### *What is a Multiplication Table?*

Think of multiplication tables in primary school. You memorise the answers to 3 x 4, 7 x 8 and so on. All the answers for digits 1 to 9 are written in a table.

Cryptography uses different rules for multiplication: multiplication with integers mod n; multiplication with polynomials mod an irreducible polynomial, but the idea is the same. The aim is to create a table that can be memorised, but this time memorised by a computer (stored in the computer memory).