CS 402 Cryptography

Problem Sheet 4

(1) A network of investors and stockbrokers is using a public key cryptosystem. The investors fear that their stockbrokers will buy stocks without investors' authorisation (to gain commission) and then, when an investor's money is lost, claim they had received instructions to buy (producing as evidence an encrypted message, saying it had come from an investor). On the other hand, the stockbrokers fear that when they buy according to an investor's instructions and the stock loses money, the investor will claim the instruction was sent by an impostor or by the broker himself. Explain how these difficulties can be resolved using the principles of public key cryptography.

(2) Let $n = pq$, where p and q are different primes, and let e be an integer coprime to $\varphi(n)$. Explain why there is an integer d such that $ed \equiv 1 \mod \varphi(n)$. Using Fermat's Little Theorem, prove that $b^{ed} \equiv b \mod n$ for any integer b.

(3) Suppose the alphabet

$$\mathrm{A}, \ldots, \mathrm{Z}, \square, ., ?, \$, 0, \ldots, 9$$

is used for all plaintexts and ciphertexts in an RSA cryptosystem. Suppose plaintext message units are length 2 and ciphertexts units are length 3.

(a) A user A has public key $(n_A, e_A) = (2047, 179)$. Encrypt for transmission to A the message SEND$\square$\$7500

(b) Break this RSA cryptosystem by factoring n_A and then computing the decryption key (n_A, d_A).

(c) Explain why, even without factoring n_A, a cryptanalyst would find d_A quickly. In other words, give reasons as to why 2047 is a bad choice for n_A.

(4) Suppose in an RSA cryptosystem plaintext and ciphertext units are length 3. However, plaintexts are written in the 27-symbol alphabet consisting of $\mathrm{A}, \ldots, \mathrm{Z}, \square$ whereas ciphertexts are written in the 28-symbol alphabet formed by adding "/" to the 27-symbol alphabet. Each user A chooses n_A between 27^3 and 28^3, so that a plaintext unit corresponds to a residue P mod n_A, and then $C \equiv P^{e_A} \mod n_A$ corresponds to a ciphertext unit.

(a) If your decryption key is $(n, d) = (21583, 20787)$ decrypt the message YSNAUOZHXXH$\square$

(b) If in part (a) you know that $\varphi(n) = 21280$, find (i) $e \equiv d^{-1} \mod \varphi(n)$, and (ii) the factorisation of n.