Information Security – Midterm
Time allowed: 45min

Dr. Van K. Nguyen

Hanoi University of Science and Technology

*Per each student, let **X** be the number determined by the last two digits of your Student Number (e.g. SN=* 1234567890 ➔ **X**=90).
*Also, let **Y = X mod 4**.*

1. Cryptanalysis

A language has an alphabet of only 4 letters with frequencies as follow: P_a=40%, P_b=20%, P_c=10% and P_d=30%. Create an encryption function from this alphabet {a,b,c,d} into the set of numbers 0-9 to make this encryption scheme become the hardest to cryptanalyze. Explain your idea.

2. RSA cryptosystem

Let k be Y*2+1

You are asked to construct an RSA public key through the following steps

1) Construct public key for e being the minimum appropriate natural number and n=p*q where p and q are selected from the range (10+k, 20+k)
2) Find the corresponding private key d (use the extended GCD algorithm for higher grade)
3) Find the ciphertext of M = 00010001 $\oplus$ (N mod 16)
4) How can you send message M securely as well as authentically.

3. MAC code

Assume that H is a cryptographic hash function with output size (Y+2)*16 bits. Assume that Scorpion-***i*** (***i***=1-9) is a specifically designed line of hardware chips for computing H, where Scorpion-***i*** can create $10^{\boldsymbol{i}}$ * 1000 hash values a second (e.g. Scorpion-2 can do 100,000 hashes/sec). This product line is the best, fastest and affordable, in the market, priced at $\boldsymbol{i}^{\boldsymbol{i/2}}$ *$1000 (e.g $2000 for *i*=2, $16000 for *i*=4).

The computer host of a bank center is connected to 100 branches which have to constantly report to the host by sending numerous datafiles of 3 specialized formats A, B and C with fixed sizes of 1200, 1500 and 1800 bytes, respectively. The data is sent in packets of size 128 bytes, including a MAC code computed using the Scorpion chips mentioned. The bank host is expected to receive up to (Y+1)*100Gbytes data per hour with at least 50% in C-datafiles. At least how much the bank needs to invest on the Scorpion chips ?