Multiple-choice test

(1 pt) Divide the following functions into one-to-one and many-to-one (multiple inputs giving the same output):

A. SHA-1  
B. Twofish in the ECB mode  
C. HMAC based on MD5  
D. RSA signature with the PKCS v.1.5 padding  
E. encryption based on the hash function RIPEMD-160

2. (1 pt) Using OAEP (Optimal Asymmetric Encryption Padding) before the RSA encryption protects against the following attacks:

A. superencryption attack  
B. encrypting a set of most likely messages with the public key, and comparing the result with the ciphertext  
C. factoring the modulus $N$ using the General Number Field Sieve Method  
D. short message attack ($e=3$, $M<N^{1/3}$)  
E. factoring the modulus $N$ using Pollard’s p-1 method

3. (1.5 pt) Match each RSA modulus $N$ with the most efficient currently known method of factoring a number of the given form and size:

A. $N=P\cdot Q$, where $P = 2^{512}+1$, Q - 50 decimal digit prime  
B. $N=P\cdot Q$, where $P$ - 55 decimal digit prime, Q - 95 decimal digit prime  
C. $N=P\cdot Q$, where $P$ - 25 decimal digit prime, Q - 175 decimal digit prime  
D. $N=P\cdot Q$, where $P$ - 50 decimal digit prime, Q - 55 decimal digit prime  
E. $N=P\cdot Q$, where $P = 2^{127}-1$, Q - 50 decimal digit prime

a. GNFS - General Number Field Sieve  
b. QS - Quadratic Sieve  
c. Pollard’s p-1 method  
d. ECM - Elliptic Curve Method  
e. Cyclotomic Polynomial Method
4. (1.5 pt) Rank the following transformations according to their speed in software starting from the fastest one:
A. DES in the CFB mode with j=32
B. DESX in the counter mode with j=16
C. Triple DES in the OFB mode with j=64
D. AES-Rijndael in the CBC mode
E. AES-Rijndael in the CFB mode with j=64

5. (1 pt) The number of bases $a \ (1 \leq a \leq n)$ for which the Fermat’s probabilistic primality test returns the result 'probably prime' for the Carmichael number $n = 561 = 3 \cdot 11 \cdot 17$ is
A. 1
B. 241
C. 320
D. 560
E. 561
Short problems

1. (3 pt) Sign the following "mini-RSA" message $M$ using the Chinese Remainder Theorem. Message: $M=33$, private key components: $d=13$, $p=5$, $q=11$.

1. (3 pt) Put the following transformations in order according to their execution time in hardware (start from the transformation that takes the smallest amount of time). Justify your answer by deriving and comparing equations for the execution times of all transformations.

A. RSA public-private key generation with the modulus $N$ length 768 bits.
B. RSA encryption with $e=3$, and the modulus $N$ length 1536 bits.
C. RSA signature generation using CRT with the 768-bit $d$, 384-bit $p$, and 384-bit $q$.
D. RSA signature verification with $e=F_4=2^{16}+1$, and the modulus $N$ length 768 bits.
E. Diffie-Hellman public-private key generation with the modulus $p$ length 768 bits, and a random 768-bit private key $x$.

2. (3 pt) Determine an average total time necessary to find a prime number of the size of 500 bits, in software, with the probability of error smaller than $2^{-85}$, under the following assumptions:

a. incremental search with a random starting point is used to screen through the candidate numbers
b. each odd number is tested first using a trial division by all primes smaller than 1500; the time of the trial division by all small primes in this set is equal (on average) to $t_D = 3 \mu s$
c. each number not rejected using the trial division is tested using the Miller-Rabin test.
d. The time of a single modular multiplication of numbers of the size 500-bits is $t_{\text{mod}}(k=500) = 0.5 \mu s$. 