(Bonus) Quiz #1

MATH 481/581 — Cryptography
Friday, March 15

Please print your name:

Problem 1. (2+4 points) Consider the finite field GF(2^6) constructed using x^6+x+1.

(a) The product of x^5+x^4 and x^5 in GF(2^6) is $\boxed{}$.

(b) The inverse of x^3 in GF(2^6) is $\boxed{}$.

Use the extra sheet for your computations. Make sure to check your answer! You have plenty of time.

Solution.

(a) $(x^5+x^4)x^5 = x^{10}+x^9$

By long division modulo 2, we find that $x^{10}+x^9 = (x^4+x^3)(x^6+x+1)+(x^5+x^3)$.

Hence, $(x^5+x^4)x^5 = x^5+x^3$ in GF(2^6).

(b) We use the extended Euclidean algorithm, and always reduce modulo 2:

$$\begin{aligned} \boxed{x^6+x+1} &\equiv x^3 \cdot \boxed{x^3} + \boxed{x+1} \\ \boxed{x^3} &\equiv (x^2+x+1) \cdot \boxed{x+1} + \boxed{1} \end{aligned}$$

Backtracking through this, we find that Bézout's identity takes the form

$$\begin{aligned} 1 &\equiv 1 \cdot \boxed{x^3} + (x^2+x+1) \cdot \underbrace{\boxed{x+1}}_{\equiv \boxed{x^6+x+1} + x^3 \cdot \boxed{x^3}} \\ &\equiv (x^5+x^4+x^3+1) \cdot \boxed{x^3} + (x^2+x+1) \cdot \boxed{x^6+x+1} \end{aligned}$$

Hence, $(x^3)^{-1} = x^5+x^4+x^3+1$ in GF(2^6). □

Problem 2. (2 points) The primitive roots modulo 14 are $\boxed{}$.

Again, use the extra sheet for your computations.

Solution. Since $\phi(14)=6$, the possible orders of residues modulo 14 are $1,2,3,6$. Residues with order 6 are primitive roots. We will find one primitive root (by trying $3,5,\ldots$) and use that to compute all primitive roots.

$3^2 \not\equiv 1$, $3^3 \equiv -1 \not\equiv 1 \pmod{14}$, so that 3 (has order 6 and hence) is a primitive root.

Every other invertible residue is of the form 3^x, and the order of $3^x \pmod{14}$ is $\frac{6}{\gcd(6,x)}$.

Since $\gcd(6,x)=1$ for $x=1,5$, the primitive roots modulo 14 are $3^1=3$ and $3^5 \equiv 5$. □

Armin Straub
straub@southalabama.edu

Problem 3. (6 points) Fill in the blanks.

(a) DES has a block size of $\boxed{}$ bits, a key size of $\boxed{}$ bits and consists of $\boxed{}$ rounds.

(b) Suppose we are using 3DES with key $k=(k_1,k_2,k_3)$, where each k_i is an independent DES key.

Then m is encrypted to $c=\boxed{}$. The effective key size is $\boxed{}$ bits.

(c) AES-128 has a block size of $\boxed{}$ bits, a key size of $\boxed{}$ bits and consists of $\boxed{}$ rounds.

(d) AES-256 has a block size of $\boxed{}$ bits, a key size of $\boxed{}$ bits and consists of $\boxed{}$ rounds.

(e) The four layers of AES are $\boxed{}$.

(f) If $x \pmod N$ has (multiplicative) order k, then x^{10} has order $\boxed{}$.

Solution.

(a) DES has a block size of 64 bits, a key size of 56 bits and consists of 16 rounds.

(b) m is encrypted to $c=E_{k_3}(D_{k_2}(E_{k_1}(m)))$.

The effective key size is 112 bits (because of the meet-in-the-middle attack).

(c) AES-128 has a block size of 128 bits, a key size of 128 bits and consists of 10 rounds.

(d) AES-256 has a block size of 128 bits, a key size of 256 bits and consists of 14 rounds.

(e) The four layers of AES are: ByteSub, ShiftRow, MixCol, AddRoundKey.

(f) If $x \pmod N$ has (multiplicative) order k, then x^{10} has order $k/\gcd(k,10)$. $\square$

Armin Straub
straub@southalabama.edu