Problem Set 2
Introduction to Modern Cryptography
Coursera-Course (Winter 2017)

Bauhaus-Universität Weimar, Chair of Media Security
Problem Session: Eik List, Course: Prof Dan Boneh, Stanford University.
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/`

Due Date: Friday, 12 Jan 2018, 1:30 PM, via email to `eik.list(at)uni-weimar.de`.

Question 1 – Parallel MACs (2+2 Points)
Let $E : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ be a secure block cipher and $K \in \{0,1\}^k$ a secret key. We denote an ℓ-block message as $M = M_1, \ldots, M_\ell$. For each of the following MACs, show why they are secure or show an efficient forgery attack:

a) $MAC'_K(M) := \bigoplus_{i=1}^{\ell} E_K(M_i)$.

b) $MAC'_K(M) := \bigoplus_{i=1}^{\ell} E_{K \oplus i}(M_i)$, (this means each block uses a different key).

Question 2 – Collision-Resistance (1+2 Points)
Say, Alice and Bob communicate a lot with each other. Their messages are all encrypted with CBC, all under the same secret fixed key. Say Eve is a passive eavesdropper who sees all ciphertexts. We call *a collision* the event that two arbitrary blocks i and j of any two arbitrary ciphertexts C^a and C^b are equal : $C^a_i = C^b_j$, with $(i,j) \neq (a,b)$.

a) Assume such a collision occurred. Which information can Eve obtain about the relation between C^a_{i-1}, C^b_{j-1} M^a_i, and M^b_j?

b) After how many blocks (summed over all ciphertexts) will a collision occur with significant probability, according to the birthday paradox? After how many encrypted blocks in total will the probability be $\geq 1/2$?

Question 3 – Euler and Fermat (3 Points)
Recall Euler's and Fermat's Little Theorem and Euler's Totient function. Then calculate:

a) $\varphi(16)$, $\varphi(19)$, and $\varphi(22)$.

b) $5^{(5^5)} \bmod 14$ and $5^{(5^5)} \bmod 13$.

c) $2^{600000} \bmod 13$ and $2^{113451345501} \bmod 101$.

Question 4 – Generators (3 Points)

a) Is 4 a generator in $\mathbb{Z}_{11}^*$? Find the discrete logarithm $\text{Dlog}_4(7)$ in $\mathbb{Z}_{11}^*$.

b) Is 6 a generator in $\mathbb{Z}_{11}^*$? Find the discrete logarithm $\text{Dlog}_6(4)$ in $\mathbb{Z}_{11}^*$.

c) What is the order of $p-1$ in $\mathbb{Z}_p^*$?

Question 5 – Diffie-Hellman Key Exchange (1+1+1+2 Points)
Alice and Bob want to exchange keys with the Diffie-Hellman protocol. They agree on a large prime p and a generator $g \in \mathbb{Z}_p^*$. Suppose that $p-1$ has only two prime factors $p-1 = m \cdot q$, where q is prime and m is small.
An active adversary Eve intercepts $A = g^a \bmod p$ from Alice and $B = g^b \bmod p$ from. Instead of A and B, Eve sends $A' = A^q \bmod p$ to Bob and $B' = B^q \bmod p$ to Alice, respectively.

a) Show that Alice and Bob still would agree on a common key K.

b) How many different keys would Eve have to test at most to find the correct one? (Hint: $|\langle g^i \rangle| = \frac{|\langle g \rangle|}{gcd(i, |\langle g \rangle|)}$.)

c) In general, would choosing $g = p-1$ be a good idea? Explain why or why not.

d) In general, one should not choose g as a generator of $\mathbb{Z}_p^*$. Show that, given g, p, A, and B, an adversary can learn if K is a quadratic residue or not.

Question 6 – Key Lengths (2 Points)
Your browser offers you two options for a cipher suite to secure your communications with your bank. Which option is preferable and why?

☐ AES-CBC with 128-bit key and Diffie-Hellman with 1024-bit primes.

☐ AES-CBC with 256-bit key and Diffie-Hellman with 2048-bit primes.

☐ AES-GCM with 128-bit key and Diffie-Hellman with 3072-bit primes.

☐ AES-ECB with 256-bit key and Diffie-Hellman with 4096-bit primes.

Question 7 – Textbook ElGamal Encryption (3 Points)
Let $\mathbb{Z}_p^*$ be a cyclic group for some prime p. Let g be a generator in some subgroup of order q in $\mathbb{Z}_p^*$. Alice' auction house chooses a secret key $a \twoheadleftarrow Z_p$ and publishes as public key (g, p, A) with $A \equiv g^a \bmod p$. Bob chooses $b \twoheadleftarrow Z_p$ and encrypts his bid m as

$$B \equiv g^b \bmod p, \qquad C \equiv m \cdot A^b \bmod p,$$

and sends the ciphertext (B, C) to Alice. Show that an adversary Eve can intercept and replace Bob's ciphertext with a valid ciphertext (B', C') of a higher bid m'. This shows that textbook ElGamal does not provide chosen-ciphertext security.

Question 8 – RSA with Small Exponents (5 Points)
Anna wants to submit an important message P encrypted with to three of her friends – Alice, Bob, and Charlie. Their public RSA keys are $(n_a, e_a) = (221, 3)$ for Alice, $(n_b, e_b) = (209, 3)$ for Bob and $(n_c, e_c) = (161, 3)$ for Charlie. Alice calculates and transmits the ciphertexts $C_a = 102$, $C_b = 53$, and $C_c = 28$. Recall the Chinese remainder theorem and reconstruct the plaintext P. Explain your computation in comprehensible manner.

Question 9 – Textbook RSA for Signatures (4 Points)
Let n be Alice' RSA modulus, d her private, and e her public key. The textbook RSA signature scheme is defined as

$$\text{Sign}(m) := m^d \bmod n,$$
$$\text{Verify}(s, m) := \begin{cases} \text{true} & \text{if } s^e \bmod n = m, \\ \text{false} & \text{otherwise.} \end{cases}$$

Assume that Eve wants Alice to sign a message m, but Alice would never sign this very m for Eve. Though, Eve can ask Alice for the signature s' for one message m', different from m. Show how Eve could use this to forge a signature for m.

Question 10 – RSA Padding Oracle (2+1 Points)
Alice wants to send a 256-bit AES key k, RSA-encrypted with a modulus n to Bob. She proposes the following simple encryption algorithm: k is used at the least significant 256 bits, and the higher bits are simply filled up with zero bits:

$$c = (0 \ldots 0 \,\|\, k)^e \bmod n$$

a) Assume Bob's server is an oracle that decrypts an incoming message and first checks if the 0-bit padding is correct. If it is incorrect, then the server outputs an error message. Show how an adversary Eve can use this information to recover at least one bit of k from an eavesdropped ciphertext c.

b) How would you fix the decryption algorithm to not allow such attacks?