# Seminar on Security Protocols and Applications
# Final Exam

17th July 2006

- ⋆ The exam duration is 1h45'.
- ⋆ All documents are allowed.
- ⋆ No electronic device is allowed.
- ⋆ If you do not have enough space on the sheet please use a separate page with your name on and clear references: use two different sheets for the different exercises as they will be corrected separately.

LAST NAME: .....

First Name: .....

# 1 RSA-KEM

Given a constant $s_D$ which will serve as a security parameter for a DEM scheme and a constant $e$, we define the following KEM scheme:

**KEM.Gen**:
input: a security parameter $s_K$
1. pick two different prime numbers $p$ and $q$ of $\frac{s_K}{2}$ bits until $\mathsf{gcd}(e, (p-1)(q-1)) = 1$
2. set $N = pq$, $d = e^{-1} \bmod (p-1)(q-1)$
OUTPUT: a public key $(N, e)$, a private key $(N, d)$

**KEM.Enc**:
input: a public key $(N, e)$
1. generate a $s_D$-bit AES key $K$
2. compute $C_0 = K^e \bmod N$
output: $(C_0, K)$

**KEM.Dec**:
input: a private key $(N, d)$, an encapsulated key $C_0$
1. compute $K = C_0^d \bmod N$
output: $K$

1. Identify the differences with the RSA-KEM scheme.

2. We assume that $s_D = 256$ (we want to use DEM based on AES with strong security) and $s_K = 4096$ (same with RSA). We want to use $e = 3$.

   Show that an adversary can easily decrypt any $C_0$ by using the public key only.

3. We now want to use $e = 17$.

   Let $K = K_L + 2^t \cdot K_H$ with $K_L < 2^t$ and $K_H < 2^{s_D - t}$. Let $K_L^e = C_L + 2^{s_K} \cdot C_H$ with $C_L < 2^{s_K}$.

   Show that if $K_H = 0$ and if an adversary can guess $C_H$ then she can decrypt $C_0$ by using the public key only. By studying the size of $C_H$, deduce the complexity and probability of success in terms of $s_K, s_D, t, e$.

   Numerical application: apply this for $s_K = 4096$, $s_D = 256$, $t = s_K/e$ and $e = 17$.

4. We now want to use $e = 2^{16} + 1$.

   Show that the previous attack is no longer feasible.

5. Show that the proposed KEM scheme is not secure in the sense of KEM security: devise an adaptive chosen ciphertext distinguishing attack.

Why isn't this attack applicable to RSA.KEM?

LAST NAME: .....

First Name: .....

# 2 Attacks on WEP

## 2.1 FMS Attack

You are sniffing a WEP connection and want to crack the key. You're no script kiddie and want to implement the FMS attack yourself.

1. You observe that the WEP driver of the system you are attacking has a bug in the way it generates IVs. Indeed, the last byte of all IVs is always 17. Does this change the number of packets you need to sniff for the FMS attack?

2. During your sniffing session you discover that every time the IV is $\{3, 255, 17\}$ the first byte has a higher than average probability of being 0. What part of the key can you retrieve from this? What is the value of this part?

3. With the IV $\{4, 255, 17\}$ the first byte is also 0 with a higher than average probability. Can you calculate another part of the key from this value? If yes, what is its value?

4. Assume that it takes about 2'000'000 sniffed packets to break a five byte (40 bit) WEP key with a classical FMS attack. Does it take $\frac{13}{5}$ times more packets to break a 13 byte key? Explain why.

## 2.2 Dictionary Attack

We know that using the fragmentation attack we can reconstruct a full key stream for one IV by sending 34 fragments. The last phrase of the text about this attack says:

> *In practice the AP's initialise their IV to 0 and increment it by one at each frame.*

5. What is the size of the 34 fragments that you have to send to retrieve a full key stream? What is the size of the responses of the AP?

6. How many fragments would you have to send to create a dictionary of key streams that decrypts 90% of the frames if the AP indeed generates its IVs as explained in the text?

7. In reality many AP's generate random IVs. How many fragments would you have to send to be able to decrypt 90% of the traffic in that case?