

Solution Sheet 13

Cryptography and Security 2022

Solution 1 A Bad EKE with RSA

1. Since $K < 2^{128}$, we have $K^3 < 2^{384}$ which is small. So, $K^3 \bmod N = K^3$. Eve could do an exhaustive search on W to decrypt $C'_1 \parallel \dots \parallel C'_8$ to obtain some candidate values for Γ . She could then compute $\sqrt[3]{\Gamma}$. For wrong guesses for the password, this is unlikely to be an integer. For the correct w , this gives K . So, Eve recovers w and K .
2. We apply the principle of the *partition attack*: the set of valid N does not corresponds to the set of messages. Namely, the most significant and the least significant bits of N must always be 1 (since N is odd and between 2^{1023} and 2^{1024}). We could also note that $N \bmod 3 = 1$, so the set of valid N is at least $\frac{1}{8}$ of the full space. Eve could do an exhaustive search on all w , decrypt $C_1 \parallel \dots \parallel C_8$ with the trial passwords and discards all trials not satisfying the above conditions. The set of possible passwords would thus be reduced by at least a factor 8. By using k executions of the protocol, the set of possible passwords is reduced by 8^k until it contains the correct password w . For instance, if w has an entropy lower than 48 bits, $k = 16$ iterations are enough to isolate the correct password.

Solution 2 Reset Password Recovery

1. The best strategy is to test the most likely possible password, i.e. k_1 , following the algorithm
 - 1: **loop**
 - 2: reset
 - 3: test k_1
 - 4: **end loop**

The expected number of test queries is

$$\sum_{i=1}^{+\infty} i \Pr[k_1] (1 - \Pr[k_1])^{i-1} = \frac{1}{\Pr[k_1]} = 2^{-H_\infty}$$

where H_∞ is called the *min-entropy*.

For the toy distribution T , we have

$$C = \frac{a}{p}$$

2. The best strategy is to test the possible passwords by decreasing order of likelihood, i.e.
 - 1: reset
 - 2: **for** $i = 1$ to n **do**
 - 3: test k_i
 - 4: **end for**

The expected number of test queries is

$$\sum_{i=1}^n i \Pr[k_i] = G$$

which is called the *guesswork entropy*.

For the toy distribution T , we have

$$\begin{aligned} G &= \frac{p}{a} \sum_{i=1}^a i + \frac{1-p}{n-a} \sum_{i=a+1}^n i \\ &= p \frac{a+1}{2} + (1-p) \frac{n+a+1}{2} \\ &= (1-p) \frac{n}{2} + \frac{a+1}{2} \end{aligned}$$

3. For $n = 3$ and $a = 1$, the condition $\frac{p}{a} \geq \frac{1-p}{n-a}$ simplifies to $p \geq \frac{1}{3}$.

We could already look at the extreme cases with $p = \frac{1}{3}$, making T the uniform distribution with $n = 3$, and $p = 1$, making T having zero probability on k_2 and k_3 . For the uniform distribution, we have $G = 2$ and $2^{-H_\infty} = 3$. So, the strategy of Q2 is better. For $p = 1$, we have $G = 1$ and $2^{-H_\infty} = 1$. So, both strategies are equally good.

In the general case, we have

$$G = \frac{5-3p}{2}$$

and

$$2^{-H_\infty} = \frac{1}{p}$$

We have equality between G and 2^{-H_∞} if and only if $3p^2 - 5p + 2 = 0$ which have roots $p = 1$ and $p = \frac{2}{3}$. So, for $\frac{1}{3} \leq p \leq \frac{2}{3}$, G is lower, and for $\frac{2}{3} \leq p \leq 1$, 2^{-H_∞} is lower. We can propose $p = \frac{5}{6}$ for which the strategy of Q1 is better.

4. The best strategy is to test the m most likely possible passwords by decreasing order of likelihood, i.e.

```

1: loop
2:   reset
3:   for  $i = 1$  to  $m$  do
4:     test  $k_i$ 
5:   end for
6: end loop

```

Let

$$p_m = \Pr[k_1] + \dots + \Pr[k_m]$$

We define the distribution $D' = D|K \in \{k_1, \dots, k_m\}$ conditioned to $K \in \{k_1, \dots, k_m\}$. We have $\Pr_{D'}[k_i] = \frac{1}{p_m} \Pr_D[k_i]$. The distribution D' has a guesswork entropy G_m defined by

$$G_m = \frac{1}{p_m} \sum_{i=1}^m i \Pr_D[k_i]$$

The expected number of iterations of the outer loop is $\frac{1}{p_m}$. The number of tests during the last iteration is G_m . The number of tests during each of the previous iteration is exactly m . So, the expected number of tests is

$$C_1 = m \left(\frac{1}{p_m} - 1 \right) + G_m$$

Note that for $m = 1$, we have $p_1 = \Pr[k_1]$, $G_1 = 1$, and $C_1 = \frac{1}{\Pr[k_1]}$. For $m = n$, we have $p_n = 1$, $G_n = G$, and $C_n = G$.