IHDCM035 – Sécurité Informatique January, 18 2024	First Name – LAST NAME	ID

Question 1: Vrai ou Faux?

Repondez aux questions suivantes en **entourant** la bonne réponse. +1 point par bonne réponse, et -0.5 par mauvaise réponse pour cette question. +0 si pas de réponse.Une note négative a ce QCM n'est pas reportée sur une autre question de cet examen.

1. Vrai Faux Si X et Y sont des variables uniformément aléatoires, alors $Z = X||Y$ est une variable uniformément aléatoire.
2. Vrai Faux Si X, Y sont des variables uniformément aléatoire, et Z une variable aléatoire, alors $W = X \oplus Y \oplus Z$ n'est pas une variable uniformément aléatoire.
3. Vrai Faux Le chiffrement par substitution est une application bijective.
4. Vrai Faux Le chiffrement par décalage avec une clé tirée uniformément aléatoire a une propriété de chiffrement "parfait".
5. Vrai Faux Un attaquant possèdant une puissance de calcule infinie ne peut rien apprendre d'un chiffrement parfait.
6. Vrai Faux Le nombre de chiffrement distincts d'un message m est égale au nombre distinct de clés pour un chiffrement par substitution.
7. Vrai Faux Le principe de Kerckhoff établi que pour être sécurisé, un chiffrement doit manipuler des espaces suffisament grands.
8. Vrai Faux Nous pouvons chiffrer plusieurs messages avec un algorithme de chiffrement possedant une sécurité sémantique et le résultat maintient cette propriété.
9. Vrai Faux Soit l'espace des clé $\mathcal{K}$, et l'espace des messages $\mathcal{M}$, si $|\mathcal{M}| > |\mathcal{K}|$, alors il n'existe pas d'algorithme de chiffrement parfait pour $\mathcal{K}$ et $\mathcal{M}$.
10. Vrai Faux La propriété de sécurité sémantique d'un chiffrement permet à un adversaire possédant une puissance de calcule finie de distinguer deux chiffrés avec une probabilité négligeable.

IHDCM035 – Sécurité Informatique January, 18 2024	First Name – LAST NAME	ID

Question 2: Time-Memory Tradeoff

Synthetisez une comparaison des tables de Hellman avec les tables Rainbow. Pour vous aider dans votre comparaison, vous pouvez orienter votre réponse en comparant:

1. La phase de précalcul des tables de Hellman avec la phase de précalcul des tables Rainbow. Aidez-vous d'un dessin.
2. La phase d'attaque en ligne des tables Hellman avec la phase d'attaque en ligne des tables Rainbow. Aidez-vous d'un dessin.

Posez le contexte de votre explication avec une fonction non-inversible $f = SHA256$, pour des mot-de-passes de 8 lettres tout au plus, chacune representée sur 8 bits.

IHDCM035 – Sécurité Informatique January, 18 2024	First Name – LAST NAME	ID

IHDCM035 – Sécurité Informatique January, 18 2024	First Name – LAST NAME	ID

Question 3: Software Security

En supposant qu'on compile le code suivant vers une architecture 32-bits x86, et qu'on nomme le programme compilé `prog`. Supposez que les défenses modernes (non-vue en cours) sont désactivées à la compilation, comme lors des exercises vu en cours.

```c
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

static char *secret = "S";

void foo(char *str) {

  char guard = *secret;

  char buffer[24];
  strcpy(buffer, str);

  if (guard == *secret)
    return;
  else {
    printf("Uh oh! Something bad happened \n");
    exit(1);
  }
}

int main(int argc, char *argv[]) {
  if (argc > 1) {
    foo(argv[1]);
  } else {
    printf("This program should be run with an input string\n");
  }
  return 0;
}
```

1. Décrivez ce qu'il se passerait en executant ce qui suit:

   ./prog "test test testAAAAAAAAAA"

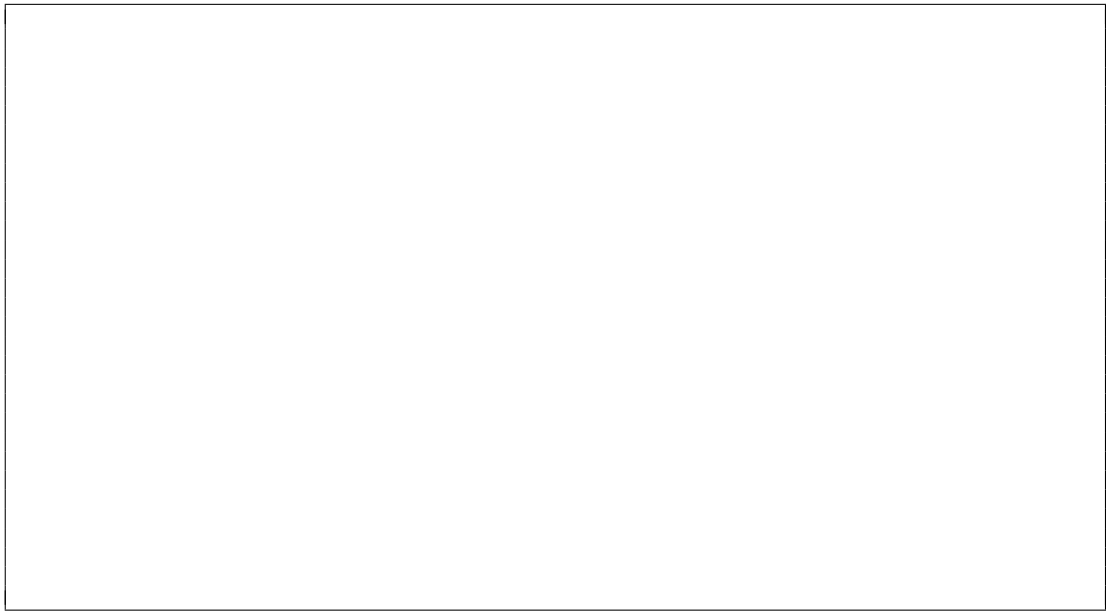
   indice: souvenez-vous que strcpy() copie aussi \0 à la destination.

2. Décrivez ce qu'il se passerait en executant ce qui suit:

   ./prog "test test testAAAAAAAAAASAAAAAAAAAAAAAAAAAAA"

3. En faisant l'hypothèse que vous n'avez pas accès au code source, mais seulement au binaire:

   - Comment pouvez-vous déterminer le secret depuis celui-ci? Expliquez l'interet apparent de ce secret dans le programme.



- En faisant l'hypothèse que le shellcode peut s'écrire simplement "shellcode", et que l'adresse du buffer sur la stack est 0xABCD à l'execution, donnez l'entrée du programme qui contourne la défense et execute le shellcode. Expliquez l'execution du programme dans la fonction foo avec un dessin de la stack.

IHDCM035 – Sécurité Informatique January, 18 2024	First Name – LAST NAME	ID