Crypto « UNPLUGGED »
Le Solitaire (Bruce Schneier)

Un atelier pour (grands) enfants
de 12 à 112 ans

@aeris / @amaelle

27 juin 2014, Pas Sage en Seine

Solitaire (Bruce Schneier)

Matériel nécessaire

- 1 jeu de 54 cartes
  - 52 cartes standard
  - 2 jokers différenciables ( & )
- Du temps. Beaucoup de temps.

Préparation des jeux

- Obtenir un certain ordre sur le 1er jeu
  - Mélange aléatoire
  - Ordre du bridge dans un journal
  - Clef secrète partagée (cf à la fin)

- Communiquer cette clef secrète à votre destinataire (Dans le cas d'un mélange aléatoire, il faut trier un 2nd jeu de manière identique au 1er et le communiquer au destinataire)

Préparation des jeux

- Dans toute la suite, le jeu est considéré comme circulaire, comme si la dernière carte était au-dessus de la première

  1 … 54 1 … 54 1 … 54 1 … 54

- L'ordre des cartes est
  - 🂡, 🂢, …, 🂪, 🂫, 🂭, 🂮
  - ♣ ♦ ♥ ♠
  - 🃟 ou 🃠 = 53

Obtenir la clef de chiffrement

- Déplacement des jokers

  - Déplacer le joker ★ de +1 rang

    … ★ X Y … → … X ★ Y …

    X … ★ → ★ X …

  - Déplacer le joker ☆ de +2 rangs

    … ☆ X Y Z … → … X Y ☆ Z …

    X Y … ☆ Z → X ☆ Y … Z

    X Y Z … ☆ → X Y ☆ Z …

Obtenir la clef de chiffrement

- Couper le jeu entre les 2 jokers

A ... B [★] C ... D [★] E ... F → E ... F [★] C ... D [★] A ... B

[★] A ... B [★] → pas de changement

A ... B [★] [★] C ... D → pas de changement

Obtenir la clef de chiffrement

- Regarder la valeur de la dernière carte

  … 🃋♦ → 🃋♦ = 24 (J = 11, ♦ = +13)

- Couper à la carte de la valeur obtenue

  1 … 24 25 … 53 🃋♦ → 25 … 53 1 … 24 🃋♦

  … 🃟★ → pas de changement

Obtenir la clef de chiffrement

- Regarder la valeur de la 1ère carte

  🂵 … → 🂵 = 31 (5 = 5, ♥ = +26)

- Regarder la valeur de la carte à cette position

  🂵 … 30 🂧 32 … 54 → 🂧

- Cette valeur correspond à une lettre
  - ♦ ♥ → 1 à 13
  - ♣ ♠ → 14 à 26
  - 🃟 ou 🃠 → ∅

  🂧 → 20 (7 = 7, ♠ = +13) → T

Chiffrement

- On boucle jusqu'à avoir collecté autant de lettres que la taille du message à chiffrer

  E X K Y S Z S G E

- On applique un chiffrement de Vigenère

  HELLO PSES

  \+ EXKYS ZSGE

  = LBVJG OLKW

- On détruit le jeu

Déchiffrement

- On applique la même formule sur le 2nd jeu pour générer la même clef de chiffrement

  E X K Y S Z S G E

- On applique un déchiffrement de Vigenère

  LBVJGOLKW

  \+ EXKYSZSGE

  = HELLOPSES

- On détruit le jeu

Partage du jeu par clef secrète

- Choisir une phrase de passe commune

  PSES IS COOL

- Convertir la phrase en chiffre

  16 19 5 19 9 19 3 15 15 12

- À partir d'un jeu trié (as … roi, ♣ ♦ ♥ ♠, 🃟🃠), on applique le solitaire en utilisant lors de la coupe les chiffres obtenus au lieu de la valeur de la dernière carte

Précautions

- Penser au déni plausible
  - Pourquoi des jeux de cartes
  - Pourquoi 2 jokers
  - Pourquoi 2 jokers différenciables (si on les marque)
- Destruction du jeu
  - Ne pas le jeter en l'air !!!
    test effectué violamment sur 2m50 avec explosion du plafond et dispersion sur 30m²
    38 cartes sur 54 (70%) toujours dans le bon ordre…
  - Le battre 6 fois correctement
- Ne jamais réutiliser le même jeu de départ
- Éviter les traces écrites
  - Le papier cigarette, c'est cool, ça brûle
- Ne pas faire d'erreur
  - La moindre erreur entraîne l'irrécupérabilité du message