ДЗ №1

№12 g) $f: \mathbb{Z}_{\varphi_n} \to Q_n$, $f(x) = x^2 \bmod n$, де $n = pq$, а p, q - великі різні прості числа, які зберігаються в секреті.

Рев: ⊕ $y = x^2 \bmod n = x^2 \bmod pq$

$\Rightarrow x = \sqrt{y} \bmod pq$ (оскільки p та q зберіг в секреті ч буд складно / неможливо)

Sec: ⊖ $y = x^2 \bmod n$, $x' \neq x$:

$f(x') = y = (x')^2 \bmod n$

$x' = -x$

$f(x) = f(-x)$

Coll: ⊖ З другої власт. можемо підібрати конкретну пару

$(x, -x)$ - колізія

$\Rightarrow$ виконується лише умова стійкості до пошуку прообразів.

№13 a)

Нехай h_1, h_2 - деякі геш-функції і $h(x) = h_1(x) \| h_2(x)$

Доведення (від супротивного)

Припустимо, $h_1(x)$ має стійкість до пошуку ~~колізії~~ колізії, а $h(x)$ (не) має

‼

Складно знайти пару (x, x'): $h_1(x) = h_1(x')$

Проте, легко знайти пару (x, x') таку що: $h(x) = h(x')$

‼

$h_1(x) \| h_2(x) = h_1(x') \| h_2(x')$

Але це можна розписати як $h_1(x) = h_1(x')$ та $h_2(x) = h_2(x')$

таку пару знайти складно

$\Rightarrow$ протиріччя $\Rightarrow$ h теж буде стійкою до пошуку колізій ◀

№16

Розглянемо функцію $f: V_n \to V_n$, $f(x) = x \oplus (x >>> 1)$

а) Сам: ⊖ Нехай $x = 0101$ та $x' = 1010$

$x >>> 1 = 1010$ $\quad x' >>> 1 = 0101$

$f(x) = 1111$ $\quad f(x') = 1111$

Знайдемо таку пару (x, x'), що $f(x) = f(x')$

Якщо треба бінарним ~~конкретним~~ загальний контрприклад можна розглянути пару $(x, \bar{x})$.

б) Опишемо правила за якими будуть висуватись на функція

$$\oplus \begin{array}{c} x_1 x_2 x_3 \dots x_n \\ x_n x_1 x_2 \dots x_{n-1} \end{array} \Rightarrow \begin{array}{c} y_1 y_2 y_3 \dots y_n \end{array}$$

$y_1 = x_1 \oplus x_n$

$y_2 = x_2 \oplus x_1$

$\vdots$

$y_n = x_n \oplus x_{n-1}$

Були намагання оцінити множину можливих значень

$|f(x)| \leq \frac{|V_n|}{2} = 2^{n-1}$, щоб дати оцінку $|f(x)| \geq 2^{n-1}$ я намагався застосувати метод мат. індукції.

Роздуми були наступні:

1) База індукції

Розглянемо $n = 2$

$x = \{00, 01, 10, 11\}$

$f(x) = \{00, 11\}$

$|f(x)| = 2^{2-1} = 2$

$$\oplus \begin{array}{c} 00 \\ 00 \end{array} \quad \oplus \begin{array}{c} 01 \\ 10 \end{array} \quad \oplus \begin{array}{c} 10 \\ 01 \end{array} \quad \oplus \begin{array}{c} 11 \\ 11 \end{array}$$

$$00 \qquad 11 \qquad 11 \qquad 00$$

2) Крок індукції

Нехай, вірно

$x_1 x_2 x_3$

$\oplus \; x_k x_1 x_2$

Далі не

в) $y_1 =$

$y_2 =$

$\vdots$

$y_n =$

Розгля

x_1

x

В р

ми о

що м

Про

2) Крок індукції

Нехай, вірне для k, тоді вірне для $k+1$

$$\left.\begin{array}{l} x_1 x_2 x_3 \dots x_k \\ \oplus\ x_k x_1 x_2 \dots x_{k-1} \end{array}\right) \text{ — ідентичні } \left.\begin{array}{l} \oplus\ x_1 x_2 x_3 \dots x_k \\ x_{k+1} x_1 x_2 \dots x_{k-1} \end{array}\right) x_{k+1} \; x_k$$

Далі незрозуміло ☺

в) $$\left.\begin{array}{l} y_1 = x_1 \oplus x_n \\ y_2 = x_2 \oplus x_1 \\ \vdots \\ y_n = x_n \oplus x_{n-1} \end{array}\right\} \Rightarrow \begin{array}{l} x_1 = y_1 \oplus x_n \\ x_2 = y_2 \oplus x_1 \\ \vdots \\ x_n = y_n \oplus x_{n-1} \end{array}$$

Розглянемо два випадки, коли $x_n = 0$ та $x_n = 1$

$x_n = 0$:

$$x_1 = y_1$$
$$x_2 = y_2 \oplus y_1$$
$$\vdots$$
$$x_{n-1} = y_{n-1} \oplus \dots \oplus y_1$$
$$x_n = y_n \oplus y_{n-1} \oplus \dots \oplus y_1$$

$x_n = 1$:

$$x_1 = y_1 \oplus 1$$
$$x_2 = y_2 \oplus y_1 \oplus 1$$
$$\vdots$$
$$x_{n-1} = y_{n-1} \oplus \dots \oplus y_1 \oplus 1$$
$$x_n = y_n \oplus y_{n-1} \oplus \dots \oplus y_1 \oplus 1$$

В результаті, маючи лише послідовність бітів з виходу (y), ми отримуємо дві послідовності x та $\bar{x}$. Єдина проблема, що ми не можемо і x розпізнати, що з цього було x, а що $\bar{x}$.

Проте, ми знайшли прообраз $\Rightarrow P_{re} : \ominus$

№17

Розглянемо функцію $f: V_n \to V_n$, $f(x) = x \oplus (x >>> 2)$

а) Coll: ⊕ Нехай $\in x = 0101$ та $x' = 1010$

$x >>> 2 = 0101$ $\quad x' >>> 2 = 1010$

$f(x) = 0000$ $\quad f(x') = 0000$

б) Оскільки правила, за якими буде вилучуватись це функція

$$\begin{array}{r} x_1\, x_2\, x_3 \ldots x_{n-1}\, x_n \\ \oplus\ x_{n-1}\, x_n\, x_1 \ldots x_{n-3}\, x_{n-2} \\ \hline y_1\, y_2\, y_3 \ldots y_{n-1}\, y_n \end{array} \Rightarrow$$

$y_1 = x_1 \oplus x_{n-1}$

$y_2 = x_2 \oplus x_n$

$y_3 = x_3 \oplus x_1$

$\vdots$

$y_{n-1} = x_{n-1} \oplus x_{n-3}$

$y_n = x_n \oplus x_{n-2}$

в) Пластина вилучення з попереднього прикладу не працює, адже немає залежності між сусідніми компонентами послідовності бітів.

$y_1 = x_1 \oplus x_{n-1}$

$y_2 = x_2 \oplus x_n$

$y_3 = x_3 \oplus x_1$

$\vdots$

$y_{n-1} = x_{n-1} \oplus x_{n-3}$

$y_n = x_n \oplus x_{n-2}$

$x_1 = y_1 \oplus x_{n-1}$

$x_2 = y_2 \oplus x_n$

$x_3 = y_3 \oplus x_1$

$x_4 = y_4 \oplus x_2$

$\vdots$

$x_{n-1} = y_{n-1} \oplus x_{n-3}$

$x_n = y_n \oplus x_{n-2}$

Аналогічно тут не вийде.

№110.

б) Потрібно знайти такий розмір вибірки r_2, за якого

$$P_2\{X_1 \cap X_2 \neq \varnothing\} \geq p$$

Тобто $1 - e^{-\frac{r_1 \cdot r_2}{N}} \geq p$

$$-e^{-\frac{r_1 \cdot r_2}{N}} \geq p - 1 \Rightarrow e^{-\frac{r_1 \cdot r_2}{N}} \leq 1 - p \Rightarrow$$

$$-\frac{r_1 r_2}{N} \leq \ln(1-p) \Rightarrow \frac{r_1 \cdot r_2}{N} \geq -\ln(1-p) \Rightarrow r_2 \geq \frac{-N\ln(1-p)}{r_1}$$

$$\Rightarrow r_2 \geq \frac{N \ln\left(\frac{1}{1-p}\right)}{r_1} \qquad \left[r_2 \approx \frac{N}{r_1} \ln\left(\frac{1}{1-p}\right)\right]$$

в) Якщо $r_1 = r_2 = \sqrt{N}$:

$$P_2\{X_1 \cap X_2 \neq \varnothing\} \geq 1 - e^{-\frac{\sqrt{N}\sqrt{N}}{N}} \Rightarrow P_2\{X_1 \cap X_2 \neq \varnothing\} \geq 1 - e^{-1}$$

Отже, $e^{-1} \approx 0{,}3679$, тобто $P_2\{X_1 \cap X_2 \neq \varnothing\} \geq 1 - 0{,}3679 =$

$= 0{,}6321$

Якщо $r_1 = r_2 = 2\sqrt{N}$:

$$P_2\{X_1 \cap X_2 \neq \varnothing\} \geq 1 - e^{-\frac{2\sqrt{N} \cdot 2\sqrt{N}}{N}} \Rightarrow P_2\{X_1 \cap X_2 \neq \varnothing\} \geq$$

$$\geq 1 - e^{-\frac{4N}{N}} = 1 - e^{-4}$$

Отже, $e^{-4} \approx 0{,}0183$, тобто $P_2\{X_1 \cap X_2 \neq \varnothing\} \geq 1 - 0{,}0138 =$

$= 0{,}9817$

№1.11.

а) „Атака дів народжень"

$$P_2\{\text{успіху}\} \approx 1 - e^{-\frac{1}{356} \cdot \frac{11(11-10)}{2}} = 1 - e^{-\frac{55}{356}} \approx 0,143$$

б) Атака Ювала

$$P_2\{\text{успіху}\} \approx 1 - e^{-\frac{11 \cdot 11}{356}} = 1 - e^{-\frac{121}{356}} \approx 0,288$$

в) Випадковий пошук прообразу

$$P_2\{\text{успіху}\} \approx 1 - e^{-\frac{11}{356}} \approx 0,03$$

Для 15 дітей:

а) $P_2\{\text{успіху}\} \approx 1 - e^{-\frac{1}{356} \cdot \frac{15 \cdot 14}{2}} \approx 0,255$

б) $P_2\{\text{успіху}\} \approx 1 - e^{-\frac{15 \cdot 15}{356}} \approx 0,468$

в) $P_2\{\text{успіху}\} \approx 1 - e^{-\frac{15}{356}} \approx 0,041$

Для 30 дітей:

а) $P_2\{\text{успіху}\} \approx 0,705$

б) $P_2\{\text{успіху}\} \approx 0,92$

в) $P_2\{\text{успіху}\} \approx 0,08$

№1.13

Розглянемо ймовірність того, що в r-вибірці не виникло колізій (серед обраних немає однакових елементів)

$$P_r\{\text{відсутня колізія}\} = \frac{N}{N}\cdot\frac{N-1}{N}\cdot\frac{N-2}{N}\cdot\ldots\cdot\frac{N-r+1}{N} = \prod_{i=0}^{r-1}\frac{N-i}{N} =$$

$$= \prod_{i=0}^{r-1}\left(1-\frac{i}{N}\right)$$

Отже, $P_r\{coll(N,r)\} = 1 - P_r\{\text{відсутня колізія}\} = 1 - \prod_{i=0}^{r-1}\left(1-\frac{i}{N}\right)$

Скористаємось наближенням $\ln(1-x) \approx -x$ для малих x

$$\ln\left(\prod_{i=0}^{r-1}\left(1-\frac{i}{N}\right)\right) = \sum_{i=0}^{r-1}\ln\left(1-\frac{i}{N}\right) \approx -\sum_{i=1}^{r-1}\frac{i}{N} = \frac{r(r-1)}{2N}$$

Отже, $\prod_{i=1}^{r-1}\left(1-\frac{i}{N}\right) \approx e^{-\frac{r(r-1)}{2N}}$

Тепер, скористаємось нерівністю $e^{-x} \le 1-\left(1-\frac{1}{e}\right)x \le 1-\frac{x}{2}$

Для $x = \frac{r(r-1)}{2N}$

$$e^{-\frac{r(r-1)}{2N}} \le 1-\left(1-\frac{1}{e}\right)\frac{r(r-1)}{2N} \le 1-\frac{r(r-1)}{4N} \Rightarrow$$

$$\Rightarrow 1-e^{-\frac{r(r-1)}{2N}} \ge \frac{r(r-1)}{4N} \checkmark$$

$$P_r coll(N,r) \ge \frac{r(r-1)}{4N}$$

Також, можемо оцінити

$$e^{-x} = 1-x+\frac{x^2}{2!}-\frac{x^3}{3!}+\ldots$$

$$e^{-\frac{r(r-1)}{2N}} = 1-\frac{r(r-1)}{2N}+\frac{\left(\frac{r(r-1)}{2N}\right)^2}{2}-\ldots$$

Отже, $1 - e^{-\frac{z(z-1)}{2N}} = 1 - \left(1 - \frac{z(z-1)}{2N} + \frac{\left(\frac{z(z-1)}{2N}\right)^2}{2} - \dots\right)$

$$1 - e^{-\frac{z(z-1)}{2N}} = \frac{z(z-1)}{2N} - \left(\frac{\left(\frac{z(z-1)}{2N}\right)^2}{2} - \dots\right)$$

Можемо сказати $1 - e^{-\frac{z(z-1)}{2N}} \leq \frac{z(z-1)}{2N}$

$$P_{2coll}(N, z) \leq \frac{z(z-1)}{2N} \checkmark$$

„або"

№ 1.4 (*) (Для випадку „[redacted]")

а) Візьмемо дві геш-функції з практики

Нехай: $h_2(x) = x$, а $h_1(x) = \text{старші } n(x)$, покладемо $n = 3$

$h_1(x) = \text{старші } 3(x)$

Нехай $\in x = 010111$ $h_2(x) = 010111$ тоді

$x' = 000111$ $h_2(x') = 000111$

$h_1(h_2(x)) = 111$

$h_1(h_2(x')) = 111$ > коліzія ◀

б) „A Graduate Course in Applied Cryptography"

Dan Boneh and Victor Shoup

Насамперед я зрозумів, що, $h(h(x))$ не буде обов'язково стійкою до попередніх колізій, навіть якщо $h(x)$ - стійка.

(Я тільки ознайомлювався)