Assignment I-Q2:

Tuesday, 24 June 2025 19:35

2 Security of pseudorandom function

Let F be a pseudorandom function, and G a pseudorandom generator with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryption in the presence of an eavesdropper and whether it is CPA-secure. In each case, the shared key is a random $k \in \{0,1\}^n$.

(a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$. (Marks 4)

(b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$. (Marks 5)

(c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 \| m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$. (Marks 6)

Total Marks: 15.

Pg 74 intro to cryptography

DEFINITION 3.21 *A private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ has* indistinguishable encryptions under a chosen-plaintext attack, *or is* CPA-

74 *Introduction to Modern Cryptography*

secure, *if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function* negl *such that*

$$\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n).$$

where the probability is taken over the randomness used by $\mathcal{A}$, as well as the randomness used in the experiment.

2a) r is some key (seed) to G

$E(r, m) = G(r) \oplus m$

① choose m_1 : $E(r, m_1) = G(r) \oplus m_1$

② choose $m_1 \oplus m_2$: $E(r, m_1 \oplus m_2) = G(r) \oplus m_1 \oplus m_2$

$E(r, m) \oplus E(r, m_1 \oplus m_2) =$

①⊕②: $[G(r) \oplus m_1] \oplus [G(r) \oplus m_1 \oplus m_2] = m_2$

CPA secure?

1) We can determine the property of $E(r,m)$ for CPA

2) We can obtain the encryption and r value.

∴ Attacker can abuse r, and find the plain text m, meaning

$G(r) \oplus m \oplus G(r) = m$

Not CPA secure! And NOT CPA secure

Let B be the event of the last b bit

$P(B = b) \leq \frac{1}{2} + \epsilon$ ∴ $\epsilon \in \mathbb{R}$

$P(B = \{0,1\}^{n+1}) = 1$

∴ $\frac{1}{2} \leq \epsilon$ ⇒ 2a) is not CPA secure

Q2a) Indistinguishability =

DEFINITION 8.29 *Two probability ensembles $X = \{X_n\}_{n\in\mathbb{N}}$ and $Y = \{Y_n\}_{n\in\mathbb{N}}$ are* computationally indistinguishable, *denoted $X \stackrel{c}{\equiv} Y$, if for every probabilistic polynomial-time distinguisher D there exists a negligible function* negl *such that:*

$$\left| \Pr_{x \leftarrow X_n}[D(1^n, x) = 1] - \Pr_{y \leftarrow Y_n}[D(1^n, y) = 1] \right| \leq \mathsf{negl}(n).$$

Let X, Y be two distributions on the encryption algo; Since r is chosen to be uniform, then r is basically random,

∴ $P\left(D(1^n, x) = 1\right) = \frac{1}{2}$ likewise $P\left(D(1^n, x) = 1\right) = \frac{1}{2}$

$x \leftarrow X_n$ $y = Y_n$

∴ According to definition 8.29

$$\left[P\left(D(1^n, x) = 1\right) - P\left(D(1^n, x) = 1\right) \right] = \left[\frac{1}{2} - \frac{1}{2}\right] = 0$$

∴ The given encryption is indistinguishable

Pg 74 intro to cryptography

DEFINITION 3.21 *A private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ has* indistinguishable encryptions under a chosen-plaintext attack, *or is* CPA-

74 *Introduction to Modern Cryptography*

secure, *if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function* negl *such that*

$$\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n).$$

where the probability is taken over the randomness used by $\mathcal{A}$, as well as the randomness used in the experiment.

CPA secure :

Let $m \in M$ and c our target message to crack

$E_{nc_b}(m) = m \oplus F(k, 0^n)$

$E_{nc_b}(m_1) = m_1 \oplus F(k, 0^n)$

$E_{nc_b}(m) \oplus E_{nc_b}(m_1) = m \oplus m_1$

we know m_1 ∴ $(m \oplus m_1) \oplus m_1 = m$

and we have the target plain text

Let B be the event of the last b bit

∴ $P(B = b) \leq \frac{1}{2} + \epsilon$ ∴ $\epsilon \in \mathbb{R}$

DEFINITION 8.29 *Two probability ensembles $X = \{X_n\}_{n\in\mathbb{N}}$ and $Y = \{Y_n\}_{n\in\mathbb{N}}$ are* computationally indistinguishable, *denoted $X \stackrel{c}{\equiv} Y$, if for every probabilistic polynomial-time distinguisher D there exists a negligible function* negl *such that:*

$$\left| \Pr_{x \leftarrow X_n}[D(1^n, x) = 1] - \Pr_{y \leftarrow Y_n}[D(1^n, y) = 1] \right| \leq \mathsf{negl}(n).$$

(b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$. (Marks 5)

Q2b)

$E_{nc_b} = m \oplus F(k, 0^n)$: F is a PRF that $\mathrm{Dom}(k, \{0,1\}^n)$

$\mathrm{Ran}: \{0,1\}^n$

Let X, Y be two distributions on the Enc_b.

Note $F(k, 0^n)$ recover the key k :

∴ $P(D(1^n, x) = 1)$ $x \to x$ $P(D(1^n, y) = 1)$ $y \to y$

$$\left[P\left(D(1^n, x) = 1\right) - P\left(D(1^n, x) = 1\right) \right] = \left[\frac{1}{2} - \frac{1}{2}\right] = 0$$

$x \leftarrow X_n$ $y = Y_n$

⇒ indistinguishable

$P(B = \{0,1\}^{2n}) = \frac{1}{2} + \frac{1}{2} = 1$

$\therefore \quad \frac{1}{2} \leq \epsilon \quad \therefore$ and is not CPA secure!

(c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 \| m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $(r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1))$. (Marks 6)

pseudorandom — CPA secure + indistinguishable — OTP — OTP

$E_c = \langle r,\ m_1 \oplus F(k,r),\ m_2 \oplus F(k, r+1) \rangle$

DEFINITION 8.29 *Two probability ensembles $X = \{X_n\}_{n\in\mathbb{N}}$ and $Y = \{Y_n\}_{n\in\mathbb{N}}$ are* computationally indistinguishable*, denoted $X \overset{c}{\equiv} Y$, if for every probabilistic polynomial-time distinguisher D there exists a negligible function* negl *such that:*

$$\left| \Pr_{x \leftarrow X_n}[D(1^n, x) = 1] - \Pr_{y \leftarrow Y_n}[D(1^n, y) = 1] \right| \leq \mathsf{negl}(n).$$

Let X, Y be two distributions on E_c. Since r is uniformly random

$\therefore$ $F(k,r)$ & $F(k, r+1)$ are effectively random too

$\therefore \quad P(D(1^n, x) = 1) = \frac{1}{2} \quad P(D(1^n, y) = 1) = \frac{1}{2}$

$x \to x \qquad y \to y$

$\therefore \quad \left|\frac{1}{2} - \frac{1}{2}\right| \leq \epsilon$

$|0| \leq \epsilon \quad \therefore$ indistinguishable

DEFINITION 3.21 *A private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ has* indistinguishable encryptions under a chosen-plaintext attack*, or is* CPA-

secure*, if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function* negl *such that*

$$\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n),$$

where the probability is taken over the randomness used by $\mathcal{A}$, as well as the randomness used in the experiment.

$F(r,k), F(r+1,k)$ are effectively random

$\Rightarrow F(k,r) \oplus m_1$ is random and $F(k, r+1) \oplus m_2$ is also random

$\therefore E_{nc_E}$ is also random

Let B be the event of the last 6 bit $= 1$

$B = E_{nc_E}(k, m)$

$\therefore \quad P(B = 1^{2n}) \leq \frac{1}{2} + \epsilon \qquad \therefore \epsilon \in \mathbb{R}$

(last bit)

$P(B = 1^{2n}) = \frac{1}{2}$

$\frac{1}{2} \leq \frac{1}{2} + \epsilon$

$0 \leq \epsilon$

$\therefore$ The E_{nc} is CPA secure!