Lecture 02

Friday, 5 August 2022 9:18 PM

Recap:

Building blocks: computational problems conjectured to be hard

↳ AES, SHA etc

↳ Number Theoretic problems

Factoring

⋮

Off - syllabus

When does a

become a sui

Note: Lecture 01 was very informal and imprecise.

For eg. what is the "AES computational problem"?

what is the factoring problem?

Are we considering worst case hardness or average case hardness?

Compare to

When does a

become NP -

Prob: to prove

We will make these precise as the course proceeds, but if this informal description is bothering you at this point, please discuss with instructor after class, or during office hrs.

06/08

Lecture plan :

1. Different security definitions for encryption, and relations between them

2. Shannon's one time pad (OTP)
(and Vigenere variation where # permutations = length of msg)

3. Limitations of OTP

4. How to overcome these limitations using computational security

1. Different security definitions for encryption

Notations : Given distⁿ $\mathcal{D}$ over finite set S,
$x \leftarrow \mathcal{D}$ denotes a random element of S drawn from distⁿ $\mathcal{D}$.

$x \leftarrow S$: uniformly random element of S.

Definition 02.01

[Ravi] : Adversary should not be able to learn msg, given ciphertext

Attempt : $\forall$ adv $\mathcal{A}$, $\forall$ distⁿ $\mathcal{D}$ over $\mathcal{M}$,

$$\Pr_{\substack{k \leftarrow \mathcal{K} \\ m \leftarrow \mathcal{D}}} \left[\mathcal{A}(\mathrm{Enc}(m, k)) = m \right] \leq \max_{x \in \mathcal{M}} \Pr_{m \leftarrow \mathcal{D}} [m = x]$$

Definition 02.02

[Ashish] Adversary should not be able to learn any predicate on msg, given ciphertext

$\forall$ adv $\mathcal{A}$, $\forall$ predicates ϕ, $\forall$ distⁿ $\mathcal{D}$,

$$\Pr_{\substack{k \in \mathcal{K} \\ m \in \mathcal{D}}}\left[\mathcal{A}\left(Enc(m,k)\right) = \phi(m) \right] \leq \max_{b \in \{0,1\}} \Pr_{m \in \mathcal{D}}\left[\phi(m) = b\right]$$

Definition 02.03

[Aditya] Probability distⁿ of msg doesn't change, even after seeing encryption of msg.

$\forall$ distⁿ $\mathcal{D}$, $\forall\, x \in \mathcal{M}$, $\forall\, c \in \mathcal{C}$

$$\Pr_{m \leftarrow \mathcal{D}}\left[m = x\right] = \Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}}\left[m = x \;\middle|\; \mathcal{E}nc(m,k) = c\right]$$

SHANNON ONE TIME PAD:

$$\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$$

$$\mathrm{Enc}(m, k) = m \oplus k$$

$$\mathrm{Dec}(ct, k) = ct \oplus k$$

Correctness : $\forall m, \ \forall k,$

$$\mathrm{Dec}(\mathrm{Enc}(m,k), k) = m.$$

Does Shannon OTP satisfy Def. 02.03 ?

We need to show that for any distⁿ $\mathcal{D}$, msg. x and ciphertext c, the following holds:

$$\Pr_{m \leftarrow \mathcal{D}}[m = x] = \Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}}[m = x \mid m \oplus k = c]$$

Consider special case where $\mathcal{D}$: uniform distⁿ over $\mathcal{M}$
and $c = 00\ldots0$

LHS : $\Pr_{m \leftarrow \mathcal{D}}[m = x] = 1/|\mathcal{M}|$ (because $\mathcal{D}$ is uniform)

RHS : $\Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}}[m = x \mid \underbrace{m \oplus k = 0^n}]$ ← equivalent to saying $m = k$

$$= \frac{\Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}}[m = x \wedge m = k]}{\Pr[m = k]}$$

$$\Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}} [m = k] .$$

Note: $m \leftarrow \mathcal{D}$ and $k \leftarrow \mathcal{K}$ are chosen independently.

$$\Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}} [m = x \;\wedge\; m = k] = 1/|\mathcal{M}|^2$$

$$\Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}} [m = k] = 1/|\mathcal{M}| .$$

This concludes the special case.

<u>Q 02.</u> Where did we use that $c = 0^n$? How to remove this simplification?

Q02. Where did we use that $\mathcal{S}$ is uniform?
How to remove this simplification?

Definition 02.04 [Perfect Indistinguishability]

$\forall\, m_0, m_1, c \in \mathcal{C}$

$$\Pr_{k \in \mathcal{K}}\left[\mathcal{E}nc(m_0, k) = c\right] = \Pr_{k \in \mathcal{K}}\left[\mathcal{E}nc(m_1, k) = c\right]$$

OTP satisfies Def. 02.04 :

$$\Pr_{k \leftarrow \mathcal{K}} \left[\mathcal{E}nc(m_0, k) = c \right] = \Pr_{k \leftarrow \mathcal{K}} \left[m_0 \oplus k = c \right]$$

$$= \Pr_{k} \left[k = m_0 \oplus c \right] = 1/|\mathcal{K}|$$

D.I.Y : Show OTP satisfies Def. 02.03 (general).

Theorem 02.01

Def. 02.03 [Perfect secrecy] $\Longleftrightarrow$ Def. 02.04 [Perfect indistinguishability]

Proof idea :

Def. 02.03 $\Rightarrow$ Def. 02.04

 :

Def. 02.03 $\Leftrightarrow$ Def 02.04

Relation between Def. 02.01, Def. 02.02 and Def 02.03 ? Either show equivalence, or demonstrate an encryption scheme that satisfies one definition but not the other.

2. Shannon One Time Pad

$$\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^{\lambda}$$

$$\mathrm{Enc}(m, k) = m \oplus k$$

$$\mathrm{Dec}(ct, k) = ct \oplus k$$

Thm 02.02 : Shannon OTP satisfies Def 02.04 (and hence, also 02.03)

Proof idea: Fix any msg m, ciphertext c

$$\Pr_{k \leftarrow \mathcal{K}}\left[Enc(m,k) = c \right] = \Pr_{k \leftarrow \mathcal{K}}\left[m \oplus k = c \right]$$

$$\vdots$$

What happens if same key is used to encrypt two different messages?

3. Limitations of perfect secrecy :

Thm 02.03

Suppose enc. scheme satisfies Def. 02.04.

Then $|\mathcal{K}| \geq |\mathcal{M}|$.

4. Computational Secrecy :

Definition 02.05 [Perfect Indistinguishability : Ver 2]

D.I.Y : show Def. 02.04 $\iff$ Def 02.05.