CRYPTOGRAPHY - 23/09/2024

PERFECT SECURITY ANALYSIS - EXAMPLES

① CLASSIC CIPHERS.

- ALL OF THEM ARE NOT PERFECTLY SECURE.
  - FIRST OF ALL, THESE CIPHERS ARE SUCH THAT $|\mathcal{K}| < |\mathcal{M}|$, E.G.
    - IN CEASAR, $|\mathcal{K}| = 1$
    - IN SHIFT, $|\mathcal{K}| = |\Sigma|$, $|\mathcal{M}| = |\Sigma|^n$

    ⋮
  - ONE COULD DEFINE AN ADVERSARY A SUCH THA

$$\Pr\left(PrivK^{eav}_{A,\Pi}\right) > \frac{1}{2}$$

WHERE Π IS ANY CLASSIC CIPHER, E.G. IN THE MONOALPHABETIC SUBSTITUTION CIPHER ONE CAN DEFINE AN ATTACK A AS FOLLOWS

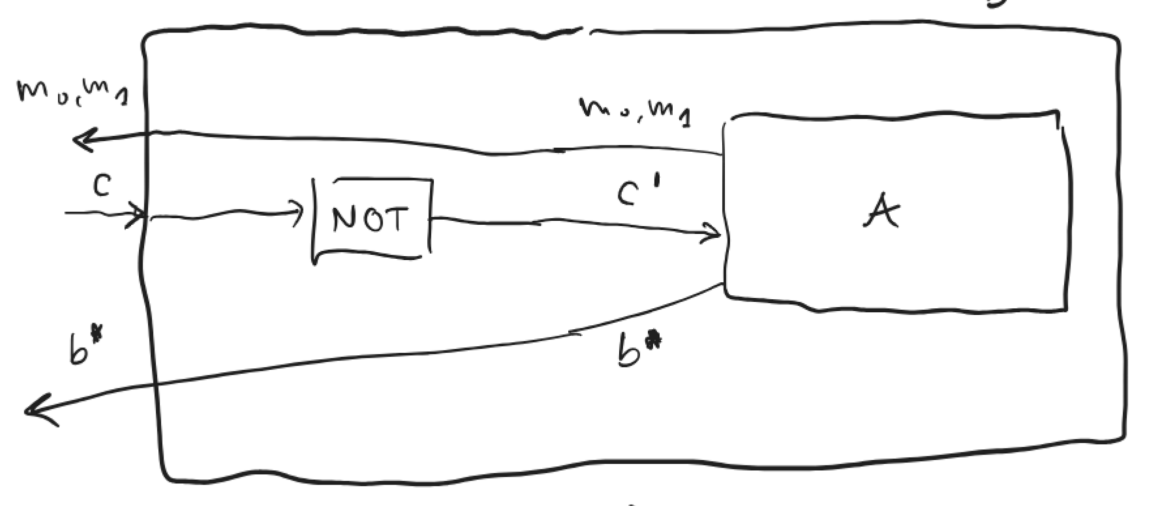
- IN THE FIRST PHASE A PRODUCES m_0, m_1 SUCH THAT $|m_0| = |m_1| = 2$ AND $m_0 = aa$ WHILE $m_1 = ab$ WHERE $a \neq b$.
- IN THE SECOND PHASE, A LOOKS AT c AND CHECKS WHETHER $c = a'a'$ OR $c = a'b'$ WHERE $a' \neq b'$. IN THE FIRST CASE IT RETURNS 0, OTHERWISE IT RETURNS 1.

② LET US CONSIDER $\Pi = (Gen, Enc, Dec)$ WHERE $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^n$, Gen IS THE SAME AS IN THE OTP, WHILE Enc IS DEFINED AS

$$Enc(k, m) = k \mathbin{\bar{\oplus}} m \qquad \begin{array}{ll} 0 \mathbin{\bar{\oplus}} 0 = 1 & 0 \mathbin{\bar{\oplus}} 1 = 0 \\ 1 \mathbin{\bar{\oplus}} 1 = 1 & 1 \mathbin{\bar{\oplus}} 0 = 0 \end{array}$$

WE CAN PROVE THAT Π IS PERFECTLY SECURE. WE USE A PROOF BY REDUCTION

FROM ANY A SUCCEEDING IN BREAKING Π $\longrightarrow$ WE GET B SUCCEEDING IN BREAKING OTP.



$$\Pr\left(PrivK^{eav}_{B,OTP} = 1\right) = \Pr\left(PrivK^{eav}_{A,\Pi} = 1\right)$$

③ A GENERALIZATION OF THE OTP:

$OTP^+ = (Gen, Enc, Dec)$ WHERE

- Gen IS AS IN OTP
- Enc IS DEFINED AS

$$Enc(k, m) = double(k) \oplus m$$

WHERE $double(d_1 \dots d_n) = d_1 d_1 d_2 d_2 \dots d_n d_n$

THIS IS INSECURE

$$|\mathcal{K}| = |\{0,1\}^n| = 2^n$$
$$\wedge$$
$$|\mathcal{M}| = |\{0,1\}^{2n}| = 2^{2n}$$

LET'S LOOK AT ATTACKS...

$m_0 = 00 \quad m_1 = 10 \quad \longrightarrow$ THE FIRST PHASE

$c = ab \quad$ IF $a = b$ THE RETURN 0 ELSE RETURN 1. $\longrightarrow$ THE SECOND PHASE

LEMMA

AN ENCRYPTION SCHEME IS PERFECTLY SECURE IFF FOR EVERY DISTRIBUTION ON $\mathcal{M}$ AND FOR EVERY PAIR OF MESSAGES $m_0, m_1 \in \mathcal{M}$, IT HOLDS THA

$$\Pr(\mathbf{C} = c \mid \mathbf{M} = m_0) = \Pr(\mathbf{C} = c \mid \mathbf{M} = m_1) \quad \forall c \in \mathcal{C}$$

PROOF

$\Rightarrow$) IT IS EASY

$$\Pr(\mathbf{C} = c \mid \mathbf{M} = m_0) = \Pr(\mathbf{C} = c) = \Pr(\mathbf{C} = c \mid \mathbf{M} = m_1)$$

$\Leftarrow$) THIS IS MORE COMPLICATED. BY HYPOTHESIS, WE KNOW THAT $\Pr(\mathbf{C} = c \mid \mathbf{M} = m_i)$ HAS THE SAME VALUE FOR EVERY m_i

$$\Pr(\mathbf{C} = c) = \sum_{m_i \in \mathcal{M}} \Pr(\mathbf{C} = c \wedge \mathbf{M} = m_i)$$

$\Pr(A \cap B) = \Pr(A \mid B) \cdot \Pr(B)$

$$= \sum_{m_i \in \mathcal{M}} \underbrace{\Pr(\mathbf{C} = c \mid \mathbf{M} = m_i)}_{\text{THESE TERMS ARE EQUAL, TO } p} \cdot \Pr(\mathbf{M} = m_i)$$

$$= \sum_{m_i \in \mathcal{M}} p \cdot \Pr(\mathbf{M} = m_i) = p \cdot \underbrace{\sum_{m_i \in \mathcal{M}} \Pr(\mathbf{M} = m_i)}_{1}$$

$$= p = \Pr(\mathbf{C} = c \mid \mathbf{M} = m)$$

⊠

THEOREM

THE OTP IS PERFECTLY SECURE

PROOF

$\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n \quad Enc(k, m) = k \oplus m \quad Dec(k, c) = c \oplus k$

- LET US FIX AN ARBITRARY DISTRIBUTION ON $\mathcal{M}$, A MESSAGE $m \in \mathcal{M}$ AND A CIPHERTEXT $c \in \mathcal{C}$.
- WHAT WE WANT TO PROVE IS THAT $\Pr(\mathbf{C} = c \mid \mathbf{M} = m)$ IS SOMEHOW INDEPENDENT ON m.

$$\Pr(\mathbf{C} = c \mid \mathbf{M} = m) = \Pr(\mathbf{M} \oplus \mathbf{K} = c \mid \mathbf{M} = m)$$

$$= \Pr(\underbrace{m \oplus \mathbf{K}}_{x} = \underbrace{c}_{y})$$

$\boxed{y = x \text{ IFF } m \oplus y = m \oplus x}$

$$= \Pr(m \oplus (m \oplus \mathbf{K}) = m \oplus c)$$

$$= \Pr((m \oplus m) \oplus \mathbf{K} = m \oplus c)$$

$$= \Pr(\mathbf{K} = m \oplus c) = 1/2^n$$

NOTABLY, $1/2^n$ DOES NOT DEPEND ON m, AND SO WE CAN CONCLUDE THAT

$$\Pr(\mathbf{C} = c \mid \mathbf{M} = m_0) = \frac{1}{2^n} = \Pr(\mathbf{C} = c \mid \mathbf{M} = m_1)$$

⊠

THEOREM (SHANNON)

IF AN ENCRYPTION SCHEME IS PERFECTLY SECURE, THEN $|\mathcal{K}| \geq |\mathcal{M}|$.

PROOF

BY WAY OF CONTRADICTION, LET US ASSUME THAT, FOR A CERTAIN P.S. ENCRYPTION SCHEME, WE HAVE $|\mathcal{K}| < |\mathcal{M}|$. SUPPOSE THAT $c \in \mathcal{C}$ IS SUCH THAT $\Pr(\mathbf{C} = c) > 0$. LET US DEFINE

$$\mathcal{M}(c) \triangleq \{\hat{m} \mid \hat{m} = Dec(k, c) \text{ FOR SOME } k \in \mathcal{K}\}$$

THE SET $\mathcal{M}(c)$ CANNOT BE TOO BIG. IN PARTICULAR, SINCE Dec IS DETERMINISTIC, IT CANNOT CONTAIN MORE THAN $|\mathcal{K}|$ MESSAGES. SO:

$$|\mathcal{M}(c)| \leq |\mathcal{K}| < |\mathcal{M}|$$

IN OTHER WORDS $\mathcal{M}(c) \subsetneq \mathcal{M}$ AND THERE IS THUS $m' \in \mathcal{M}$ SUCH THAT $m' \notin \mathcal{M}(c)$

$$\Pr(\mathbf{M} = m' \mid \mathbf{C} = c) = 0 \neq \Pr(\mathbf{M} = m')$$

THEY CANNOT HAVE THE SAME VALUE!

↓

THIS IS A CONTRADICTION

BECAUSE THERE IS NO ASSUMPTION WHATSOEVER ABOUT THE DISTRIBUTION OVER MESSAGES AND THE ENCRYPTION SCHEME IS PERFECTLY SECURE!

⊠