Perfect Secrecy

Monday, February 9, 2026 7:19 PM

Recall : one-time-pad

1] Perfect Secrecy

The scheme E is Shannon-secure when given any two plaintexts, m_1 and m_2, and a ciphertext c, then

$$\text{prob}\,(E(m_1) = c) = \text{Prob}\,(E(m_2) = c)$$

Thus, $\text{Prob}(m_1) = \text{Prob}(m_1 \mid c)$

e.g. ①

XOR scheme, $E(P, k) = P \oplus k$, for 8-bit plaintext, and 4-bit key (Vegenere' style)

$P = 1001\ 1100$
$k = 1101\ 1101$
$\oplus$
$c = 0100\ 0001$

is it Shannon-secure?

Soln. Not shannon secure for

$m_1 = 1111\ 0000$,
$m_2 = 1111\ 1111$, and $c = 0011\ 1100$

c is more likely from m_1 than m_2

② Same XOR scheme, with a random 8-bit key

that

a) start in 1 and then 7 random bits

No, for $m_1 =$ 0000 0000

$m_2 =$ 1000 1000

$c =$ 0111 1111

then c is from m_2.

b) has more 1's than 0's

No, for $m_1 =$ 1111 1111

$m_2 =$ 0000 0000

$c =$ 1111 1100

then c is more likely from m_2

c) has same number of 1's and 0's randomly

No, $m_1 =$ 1111 1111

$m_2 =$ 1010 1111

$c =$ 1010 1010

Then c is more likely from m_1

d) Purely ramdom 8-bit key

yes, it is one-time-pad

2] Application FLT

Thm: $a^{p-1} \equiv 1 \pmod{p}$

① Primality test : $n = 1003$ 1003

$2^{1002} \pmod{1003} \equiv 990 \neq 1$

$\Rightarrow$ not prime

② $n = 241$

$2^{240} \mod 241 \equiv 1$

$\Longrightarrow$ psudoprime to base 2

try another base

9 mod 103

② To find $a^{-1} \pmod{p}$

$a^{-1} \equiv a^{p-2} \pmod{p}$

e.g. $9^{-1} \equiv 9^{101} \pmod{103}$

$23 \cdot 9 \equiv 1 \pmod{103}$