Equivocation

8-bit integer

$$H(x) = -\sum_{i=1}^{2^8} \frac{1}{2^8} \log \frac{1}{2^8} = \log 2^8 = 8$$

If parity = 0

$$H(x|bit\ 8\ is\ 0) = -\sum_{i=1}^{2^7} \frac{1}{2^7} \log \frac{1}{2^7} = \log 2^7 = 7$$

Joint Probability / Uncertainty

Case 1

X = die throw, Y = coin toss

$$p(X = 3, Y = head) = p(Y = head)p(X = 3|Y = head)$$

As $p(X = 3|Y = head) = p(X = 3)$ because they are independent

$$p(X = 3, Y = head) = p(Y = head)p(X = 3) = \frac{1}{12}$$

Case 2

Toss coin

on head : 3-sided die

on tail : 6-sided die

$$p(X = 3, Y = head) = p(Y = head)p(X = 3|Y = head) = \frac{1}{2} \times \frac{1}{3} = \frac{1}{6}$$

$$p(X = 3, Y = tail) = p(Y = tail)p(X = 3|Y = tail) = \frac{1}{2} \times \frac{1}{6} = \frac{1}{12}$$

In case 1, X=3,Y=head (independent)

$$H(X|Y) = H(X) = \log 6$$

In case 2, X=3,Y=head (dependent)

$$H(X|Y) = \sum_Y p(Y) \sum_X p(X|Y) \log p(X|Y)$$

$$= p(Y = head) \sum_X p(X|Y = head) \log p(X|Y = head)$$

$$+p(Y = tail)\sum_X p(X|Y = tail)\log p(X|Y = tail)$$

$$= \frac{1}{2}\log 18$$

$H(M|C) = H(M) and p(M|C) = p(M)$ define perfect security

Key Equivocation

The uncertainty $H(K|C)$ in the key given some ciphertext

Case 1

KHOOR ZRUOG as a Caesar cipher: $\Rightarrow H(K|C) = 0$ (see handout)

Case 2

J as a Caesar cipher: $\Rightarrow H(K|C) = 1$

Formula : $H(K|C) = -\sum_C p(C)\sum_K p(K|C)\log p(K|C)$

In case 1, $p(C) = 26^{-10}$ and $p(K|C) = \begin{cases} 0 & if \quad K \neq 23 \\ 1 & if \quad K = 23 \end{cases}$

$$H(K|C) = \sum_K p(K|C)\log p(K|C) = \sum_{i=1}^{26^{10}} 26^{-10}0 = 0$$

In case 2 $p(C) = 26^{-1} and p(K|C) = \begin{cases} 0 & if \quad K \neq 9, 25 \\ \frac{1}{2} & if \quad K = 9 \\ \frac{1}{2} & if \quad K = 25 \end{cases}$

$$H(K|C) = -\sum_C p(C)\sum_K p(K|C)\log p(K|C)$$

$$= \sum_{i=1}^{26} \frac{1}{26}(\frac{1}{2}\log\frac{1}{2} + \frac{1}{2}\log\frac{1}{2}) = -\log\frac{1}{2} = 1$$

Unicity Distance

Smallest length of text N such that $H(K|C) \approx 0$

$$N = \frac{H(K)}{D} \Rightarrow H(K) - DN = 0$$

This is impossible when # of Keys = # meaningful mesg

So: $H(K) = \log 2^{RN} = RN$

RN - DN = 0

rM = 0 where R is absolute rate and r is the actual rate

Example: $CaesarH(K) = \log 26 = 4.7$ so
$N = \frac{4.7}{3.2} \approx 1.5$

Number Theory

5 = 12 mod 7
12 $\equiv_7$ 5 (Mathmatical notation)
12 = 5 + 7k

a mod n = b
Principle of modular arithmetic: mod can be moved into multiplication and addition

Examples: 7×9 mod 4
= (7 mod 4) (9 mod 4) mod 4
= 3

2^{20} mod 3 = $(2^{10})(2^{10})$ mod 3
= $(2^5)(2^5)(2^5)(2^5) mod 3$
= $(2^2 mod 3)(2^3 mod 3)(2^2 mod 3)(2^3 mod 3)(2^2 mod 3)(2^3 mod 3)(2^2 mod 3)(2^3 mod 3)(2^2 mod 3)(2^3 mod 3) mod 3$
= $[(1)(2)(1)(2)(1)(2)(1)(2)(1)(2)] mod 3$
= 16 mod 3 = 1

Solve ax mod n = 1 for any a and n (if possible)
Consider 2x mod 5 = 1. 2xmod 5 generates a complete set of residues, as

$$2(0) mod 5 = 0$$

$$2(1) mod 5 = 2$$

$$2(2) mod 5 = 4$$

$$2(3) mod 5 = 1$$

$$2(4) mod 5 = 3$$

(and so 2x mod 5 = 1 has a solution – x = 3). But 2x mod 4 will not:

$$2(0) mod 4 = 0$$

$$2(1) mod 4 = 2$$

$$2(2) mod 4 = 0$$

$$2(3) mod 4 = 2$$

(and so 2x mod 4 = 1 does not have a solution.)

Solution requires gcd(a,n) = 1 $\Rightarrow$ a, x relatively prime. $2x mod 5$ gives a complete set of residues. After removing the zero get a reduced set of residues, which is the set for which $axmodn = 1$ has a solution. Totient function ϕ is the number of elements in the reduced set of residues.

$\phi(4) = 2$
$\phi(5) = 4$
$\phi(p) = p - 1$ when p is prime

$15 = 3 \times 5 \phi(15) = 8 = 2 \times 4 = (3-1)(5-1)$
$\phi(pq)$ = pq-p-q+1 = (p-1)(q-1) when p and q is prime