(1) Cipher Modes

(2) Random Numbers

(3) Collect Project Proposals

Electronic Codebook (ECB)

$M = P_1 P_2 P_3 P_4 \ldots P_n$ → pads the last block potentially.

$C = E_K(P_1)\, E_K(P_2)\, E_K(P_3) \ldots E_K(P_n)$.

* Cipher Block Chaining (CBC)

$C_1 = E_K(P_1 \oplus IV)$

$C_2 = E_K(P_2 \oplus C_1)$

$C_3 = E_K(P_3 \oplus C_2)$

Improvement: less chance of repeated ciphertext blocks.

Can NOT be parallelized.

To Decrypt,

Decrypt C_1 to get $temp = P_1 \oplus IV$

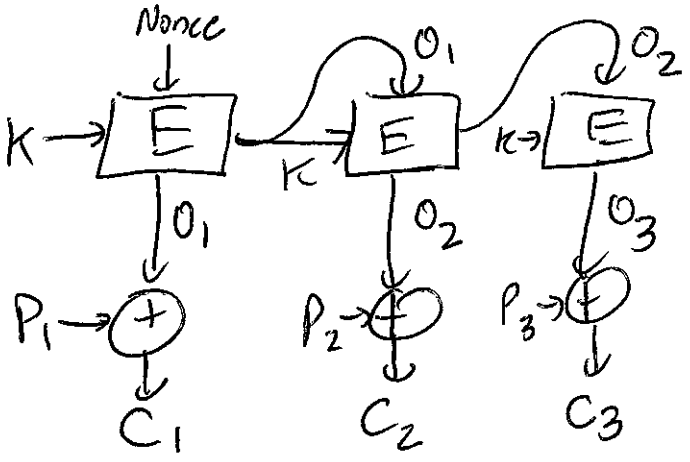
Calc $temp \oplus IV = \boxed{P_1}$

Decrypt C_2 to get $temp = P_2 \oplus C_1$

Calc $temp \oplus C_1$

$\boxed{P_2}$

Output Feedback Mode (OFB)



Random Numbers

Pseudo random #s.

Create with a "seed".

$f(s) = x_1$ LSB

$f(x_1) = x_2$ LSB

$f(x_2) = x_3$ LSB

⋮

Random Bit Test FIPS 140-1 test

(1) Generate 20,000 bits

(2) See if each of these is true

(a) #0s should be in btw 9,654 - 10,346.

(b) Calculate the frequency of 4 bit blocks

$\underbrace{b_0 b_1 b_2 b_3}\ \underbrace{b_4 b_5 b_6 b_7}\ \ldots\ [b_{19996} b_{19997} b_{19998} b_{19999}]$

let n_i = # times 4 bits = i

n_0 through n_{15} $\quad \sum_{i=0}^{15} n_i = 5000.$

$$X = \frac{16}{5000} \sum_{i=0}^{15} n_i^2 - 5000$$

$1.03 < X < 57.4$

(c) Run test $\quad$ 0001011010110

3, 1, 1, 2, 1, 1, 1, 2, 1

1	2267-2733
2	1079-1421
3	502-748
4	223-402
5	90-223
6+	90-223

Unique prime factorization

$75 = 3^1 \times 5^2$ $\quad n = \prod_{p_i \in Prime} p_i^{a_i}$

Mostly we'll either deal with primes of values of n, where $n = pq$, $p \in Prime$, $q \in Prime$.

One hard problem is FACTORING. but forward problem, multiplication, is EASY.

Fermat's Last Thm
$a^n + b^n = c^n$, no solns in pos ints $n > 2$.

Fermat's Thm

If $\gcd(a, p) = 1$ and $p \in Prime$,

Then $a^{p-1} \equiv 1 \bmod p$.

$S = \{1, 2, 3, \ldots, p-1\}$

$T = \{a, 2a, 3a, \ldots, (p-1)a\}$

$p = 7$
$a = 4$

$\{1, 2, 3, 4, 5, 6\}$

$\{4, 8, 12, 16, 20, 24\}$

$\hookrightarrow \{4, 1, 5, 2, 6, 3\}$

T mod p

The values in set S and set T are identical mod p!

(1) no value in $T \equiv 0 \pmod p$

$$T = \{ a_i \mid i \in \{1,2,\dots,p-1\} \}$$
$$i \in S$$

If p divides evenly into a term in T, then either ~~$p \mid a$~~ or ~~$p \mid i$~~.

~~$p \mid a$~~ — given $\gcd = 1$

~~$p \mid i$~~ — $0 < i < p$ so this is impossible.

(2) no 2 values in T are equivalent mod p.

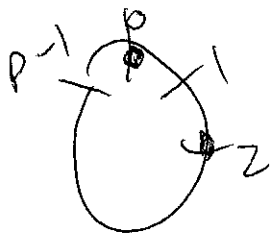
Assume 2 different terms in T are equivalent mod p:

$$a_i \equiv a_j \pmod p, \quad i \neq j$$
$$a_i - a_j \equiv 0 \pmod p \quad 0 < i, j < p.$$
$$a(i-j) \equiv 0 \pmod p$$

$\Longrightarrow$ ~~$p \mid a$~~ or ~~$p \mid (i-j)$~~

~~$p \mid a$~~ — given $\gcd = 1$

~~$p \mid (i-j)$~~ — $1 \leq |i-j| \leq p-2$ NOT POSSIBLE



$4 \times 8 \times 12 \times 16 \times 20 \times 24$

$4 \times 1 \times 4 \times 2 \times 4 \times 3 \times 4 \times 4$

$4 \times 5 \times 4 \times 6$

$= 4^6 (1 \times 2 \times 3 \times 4 \times 5 \times 6)$

$S = \{1, 2, \ldots, p-1\}$

$T = \{a, 2a, \ldots a(p-1)\}$

equiv mod p

Multiply all values in T, and S.

$$\prod_{i=1}^{p-1} ai \equiv \prod_{i=1}^{p-1} i \pmod p$$

$$a^{p-1} \prod_{i=1}^{p-1} i - \prod_{i=1}^{p-1} i \equiv 0 \pmod p$$

$$a^{p-1}(p-1)! - (p-1)! \equiv 0 \pmod p$$

$$(p-1)! \left[a^{p-1} - 1\right] \equiv 0 \mod p$$

~~$p \mid (p-1)!$~~ OR $p \mid (a^{p-1} - 1)$

$a^{p-1} - 1 \equiv 0 \mod p$

$a^{p-1} \equiv 1 \mod p$

$a = 4$

$4^1, 4^2, 4^3, 4^4, 4^5, 4^6 \mod 7$

4, 2, 1, 4, 2, 1

all cycle lengths divide evenly into $p-1$.

$3^1, 3^2, 3^3, 3^4, 3^5, 3^6 \mod 7$

3, 2, 6, 4, 5, 1

if a base "generates" all possible remainders, we will call it a generator/primitive root mod p.

$4^3 \bmod 7 = 4^2 \times 4 \bmod 7 = 2 \times 4 \bmod 7 = 1$

$3^q \equiv 5 \pmod 7$

hard to find q w/o brute force!

→ DISCRETE LOG PROBLEM

$\log_3 81 = ?$ $\quad 3^q = 81$ (We can binary search this)

Define EULER PHI FUNCTION

$\phi(n)$ = the # of values in the set $\{1, 2, 3, \ldots, n-1\}$ relatively prime to n.

$\phi(12) = 4$

gcd(1,12)=1

(2,12)

(3,12)

(4,12)

gcd(5,12)=1

gcd(7,12)=1

gcd(11,12)=1

Affine

$f(x) = (ax+b) \bmod n$

$b = \{0, 1, 2, \ldots n-1\}$

a = only values relatively prime to n.

keys = $n\phi(n)$.

$\phi(p) = p-1$ $\{1, 2, 3, \ldots p-1\}$

all are relatively prime w/ prime number p.

$\phi(p^k) = p^k - \frac{p^k}{p}$

$= p^k - p^{k-1}$

$= \boxed{p^{k-1}(p-1)}$

$p=5, k=2$

$\{1, 2, 3, 4, (5), 6, 7, 8, 9, (10), \ldots 24, (25)\}$

---

if $\gcd(a,b) = 1$ then $\phi(ab) = \phi(a) \cdot \phi(b)$.

$\phi(12) = \phi(2^2 \times 3) = \phi(2^2)\,\phi(3)$

$= (2^2 - 2^1)(3-1)$

$= 2 \times 2$

$= 4$