Pi) Fercmat's little theoriem:

Theorem:

If p is a praime and a is an integer such that gcd(a,p) = 1 then ap-1 = 1 mod p

Przoof:

consider the set 3 = 2a, 2a, 30. (P-1) als mod p Since a is copraine top, multiplication by a Perzonates the set 1, 2. P-14. 50, a. 2a... CP-1) a = 1.2-11 (P-1) mod p

that is a P-1 (p-1)! = (p-1)! mod p

Cancelling (p-1)! a P-1 = 1 mod p

Example: month submined accounts prices

compute 36 mod 7 using Ferenat's Theorems since 7 is praime and ged (3, 7)=1,

37-1 = 36 = 1 mod 7

USP IN RSA:

Used in

(P2) Fulerc's Totient Function: (

Eulen's Function: $\phi(n) = Numbere of integers \leq n$ that are coprator

compute:

 $\phi(20) = 20(1-\frac{1}{2})(1-\frac{1}{9}) = 20 \cdot \frac{1}{2} \cdot \frac{4}{9} = 8$

Theorem (Multiplicativity):

If m and n are copraine, then

Q(mn) = 6(m) Q(n)

Przoof:

-> using chinese Remainder theorem Bijection between 2xm = 2xm x 2xm

1=(1.6) pob. peus ourigid ei t. 37419

9 harres = 1 95 1(1-9) prolles mas

Percook.

93) CPT Enample:

2 = 2 mod 3 n=3 mod 4 7 = 1 mod 5

Using CPT With N = 60, N, = 20, N, = 15, N3=12

Find inverge:

-7 20-1 mod 3 = 2 10 10 starray 110 20000

-> 15 1 mod 1 = 3

-> 12-1 mod 5 = 3

Thon,

Non. n = (2.70.2) + (3.15.3) + (1.12.3) = 80 + 135 + 36 = 251n = 251 mod 60 => 2 = 11 mod 60

2 - 16 - 17 - 14

VI BOOK FROM WILLIAMS 19

94) Carzmichael Numberz:

561 = 3 X11 X 17

Check:

-7 Squarce Fitte

-7 Forz each P1561, P-11560

721560

-7101560

-7 161960

6 atis fiers korasell's cruteraion -7 561 is a currented Numberz.

95) Preimitive Root Modulo 17:

check powers of condidates

Try q=3 $3^1=3$, $3^2=9$, $3^3=10$, $3^4=13$, $3^5=5$, $3^6=15$, $3^7=1$, $3^8=16$, $3^9=14$, ...

Coverce all elements of 21/4 => 3 is a

Praimitive root mod 17

96) Discrete Logarithm:

Find x such that 32 = 13 mod 17

TITTY

731=3

73229

7 33 = 16

34 = 13 ~

50, x= 4

*1X11X & = 19,

Care michael Numbers:

D 7 3 12 8 3 16

phoener Leca .

POIS ECACH PIECE, P-11860

. 21560.

2931216

0751916

- רועל בו משח -

Knusell's

97) Discreete log in Diffie - Hellman:

TUSES Difficulty of computing discrete logarithm

-> public: p, g praivate: a,b

Frichange: A = gu mod P, B = gb mod p

-7 shured Key: god mod p mod p

& security relies on: hardness of computing

a from ga mod pro (8400) = (10) = (19)

98) Cipherz comparcison:

cloheiz	Mechanism !	KETSPULL	Frequency analysis
Substitution	Replace Letters	26'.	Vulnerable
rearsposition	Permute Posititions	Dependson length	Lux Vuinerias 6
Play fair	Digraph	25 x 25 matrum	Paratally tesistan

Plaintent: 9" HEILO " SIN - HIS " MOTHINGO 139 (8 -75ubstitution (consult shifts): "KHOOR"

-7 Transposition (block of 5): "OLLEH" -7 Plu7 Fair (Mutrain): Uses distrupts like HE, LL>

Enercypt via marriere truly.

Griden ciphen: Griven a = 5 , b = 8, planteset: "Dept of ICT, MI

a) Convert letters to numbers: D=3,E=1.

Bustadura 1212 comparay no sono a francos

Enitry p1: E(x) = (9x+8) mod 26

b) Decemption:

Invertese of 5 mod 26=21

Jamparine D(7) = 21 (7-8) mod 26

Apply to ciphercteril to get orciginal mussay
Jan 1016) Design a Novel Ciphere:

Page a

min Digressph 25x25 ...

torstered ciphen: 1) Bubstitution: Caesant Vigenerce Combination

2) perconulation. Bit-level transpose

by PANH (eg. (EPS Pl seed)) a million . WHATHO WE (S TO MIDINE) CONTINUED

Enchyphion Process

-75tep 1: Apply Caesair with trandom shift -75tep 2: Apply vigenere with fined keyword -75tep 3: Transpose using a key-generated matrin

Dectaption:

Pererose setps with inverse operations.

CTP Hanalysis:

-> Weak PANG makes personntation predictable

> vingenerce vulnercable to key length attack

-> consult training breakable if used alone.