Sponsored by

CASIO

@MEIConference #MEIConf2018

About MEI

- Registered charity committed to improving mathematics education
- Independent UK curriculum development body
- We offer continuing professional development courses, provide specialist tuition for students and work with employers to enhance mathematical skills in the workplace
- We also pioneer the development of innovative teaching and learning resources

Modular Arithmetic (working with remainders)

When working "modulo n" we are only interested in remainders

$$3 \times 5 \equiv 5 \bmod 10 \qquad 3 \times 5 \equiv ? \bmod 13$$

$$2 \times 8 \equiv 6 \bmod 10 \qquad 2 \times 8 \equiv ? \bmod 13$$

$$12 \times 18 \equiv 6 \bmod 10 \qquad 12 \times 18 \equiv ? \bmod 13$$

$$2^{10} \equiv 4 \bmod 10 \qquad 2^{10} \equiv ? \bmod 13$$

$$3 \times 7 \equiv 1 \bmod 10 \qquad ? \times 7 \equiv 1 \bmod 13$$

$$7x \equiv 8 \bmod 10? \qquad 7x \equiv 8 \bmod 13?$$

Modular Arithmetic (working with remainders)

When working "modulo n" we are only interested in remainders

$3 \times 5 \equiv 5 \mod 10$

$2 \times 8 \equiv 6 \mod 10$

$12 \times 18 \equiv 6 \mod 10$

$2^{10} \equiv 4 \mod 10$

$3 \times 7 \equiv 1 \mod 10$

$7x \equiv 8 \mod 10?$

$3 \times 5 \equiv 2 \mod 13$

$2 \times 8 \equiv ? \mod 13$

$12 \times 18 \equiv ? \mod 13$

$2^{10} \equiv ? \mod 13$

$? \times 7 \equiv 1 \mod 13$

$7x \equiv 8 \mod 13?$

Modular Arithmetic (working with remainders)

When working "modulo *n*" we are only interested in remainders

$3 \times 5 \equiv 5 \pmod{10}$ $\qquad$ $3 \times 5 \equiv 2 \pmod{13}$

$2 \times 8 \equiv 6 \pmod{10}$ $\qquad$ $2 \times 8 \equiv 3 \pmod{13}$

$12 \times 18 \equiv 6 \pmod{10}$ $\qquad$ $12 \times 18 \equiv ? \pmod{13}$

$2^{10} \equiv 4 \pmod{10}$ $\qquad$ $2^{10} \equiv ? \pmod{13}$

$3 \times 7 \equiv 1 \pmod{10}$ $\qquad$ $? \times 7 \equiv 1 \pmod{13}$

$7x \equiv 8 \pmod{10}$? $\qquad$ $7x \equiv 8 \pmod{13}$?

Modular Arithmetic (working with remainders)

When working "modulo n" we are only interested in remainders

$3 \times 5 \equiv 5 \pmod{10}$

$2 \times 8 \equiv 6 \pmod{10}$

$12 \times 18 \equiv 6 \pmod{10}$

$2^{10} \equiv 4 \pmod{10}$

$3 \times 7 \equiv 1 \pmod{10}$

$7x \equiv 8 \pmod{10}$?

$3 \times 5 \equiv 2 \pmod{13}$

$2 \times 8 \equiv 3 \pmod{13}$

$12 \times 18 \equiv 8 \pmod{13}$

$2^{10} \equiv ? \pmod{13}$

$? \times 7 \equiv 1 \pmod{13}$

$7x \equiv 8 \pmod{13}$?

Modular Arithmetic (working with remainders)

When working "modulo n" we are only interested in remainders

$3 \times 5 \equiv 5 \pmod{10}$

$2 \times 8 \equiv 6 \pmod{10}$

$12 \times 18 \equiv 6 \pmod{10}$

$2^{10} \equiv 4 \pmod{10}$

$3 \times 7 \equiv 1 \pmod{10}$

$7x \equiv 8 \pmod{10}$?

$3 \times 5 \equiv 2 \pmod{13}$

$2 \times 8 \equiv 3 \pmod{13}$

$12 \times 18 \equiv 8 \pmod{13}$

$2^{10} \equiv 10 \pmod{13}$

$? \times 7 \equiv 1 \pmod{13}$

$7x \equiv 8 \pmod{13}$?

Modular Arithmetic (working with remainders)

When working "modulo n" we are only interested in remainders

$3 \times 5 \equiv 5 \bmod 10$ $\qquad$ $3 \times 5 \equiv 2 \bmod 13$

$2 \times 8 \equiv 6 \bmod 10$ $\qquad$ $2 \times 8 \equiv 3 \bmod 13$

$12 \times 18 \equiv 6 \bmod 10$ $\qquad$ $12 \times 18 \equiv 8 \bmod 13$

$2^{10} \equiv 4 \bmod 10$ $\qquad$ $2^{10} \equiv 10 \bmod 13$

$3 \times 7 \equiv 1 \bmod 10$ $\qquad$ $2 \times 7 \equiv 1 \bmod 13$

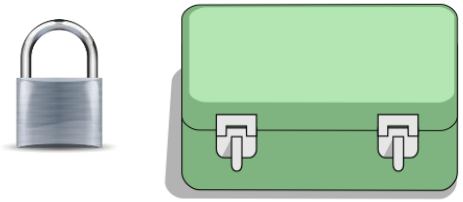
$7x \equiv 8 \bmod 10?$ $\qquad$ $7x \equiv 8 \bmod 13?$

HOW TO SHARE A SECRET

DAVID BEDFORD
KEELE UNIVERSITY
@DAVIDB52S

Ciphers

- A Cipher is a method for transforming a message so that it is unreadable to anyone except the intended recipient.
- We can think of it as a “lock”, which keeps the message safe unless the recipient has the “key”.

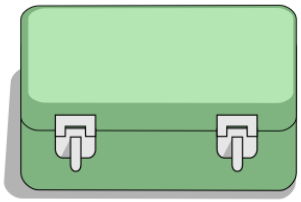


- We must protect the “key”!

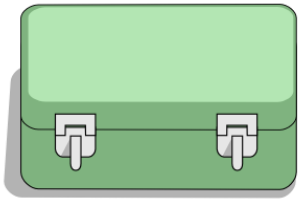
The key problem

- All the Ciphers of this form have a common problem: how do we send the key?

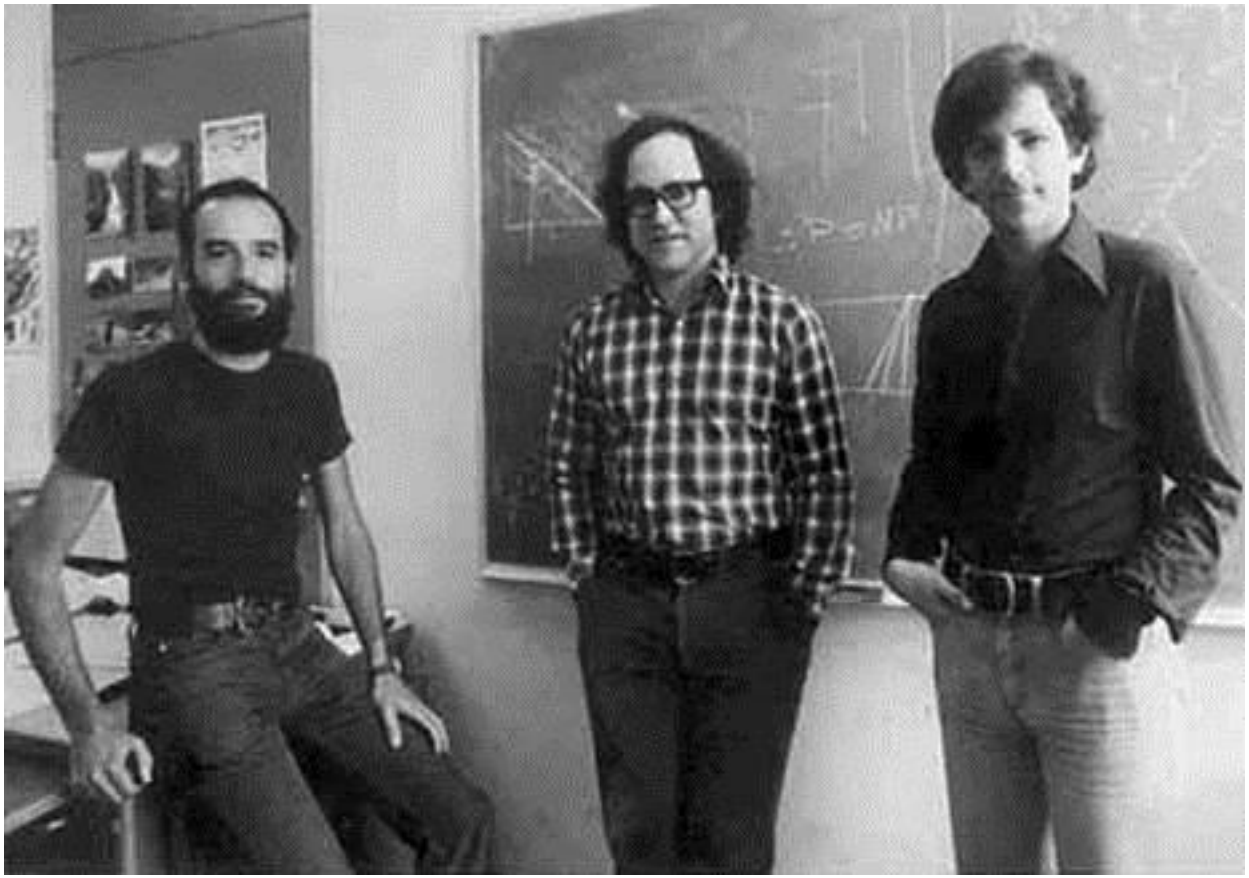
The key problem solved!



The key problem solved again!



RSA Cryptography

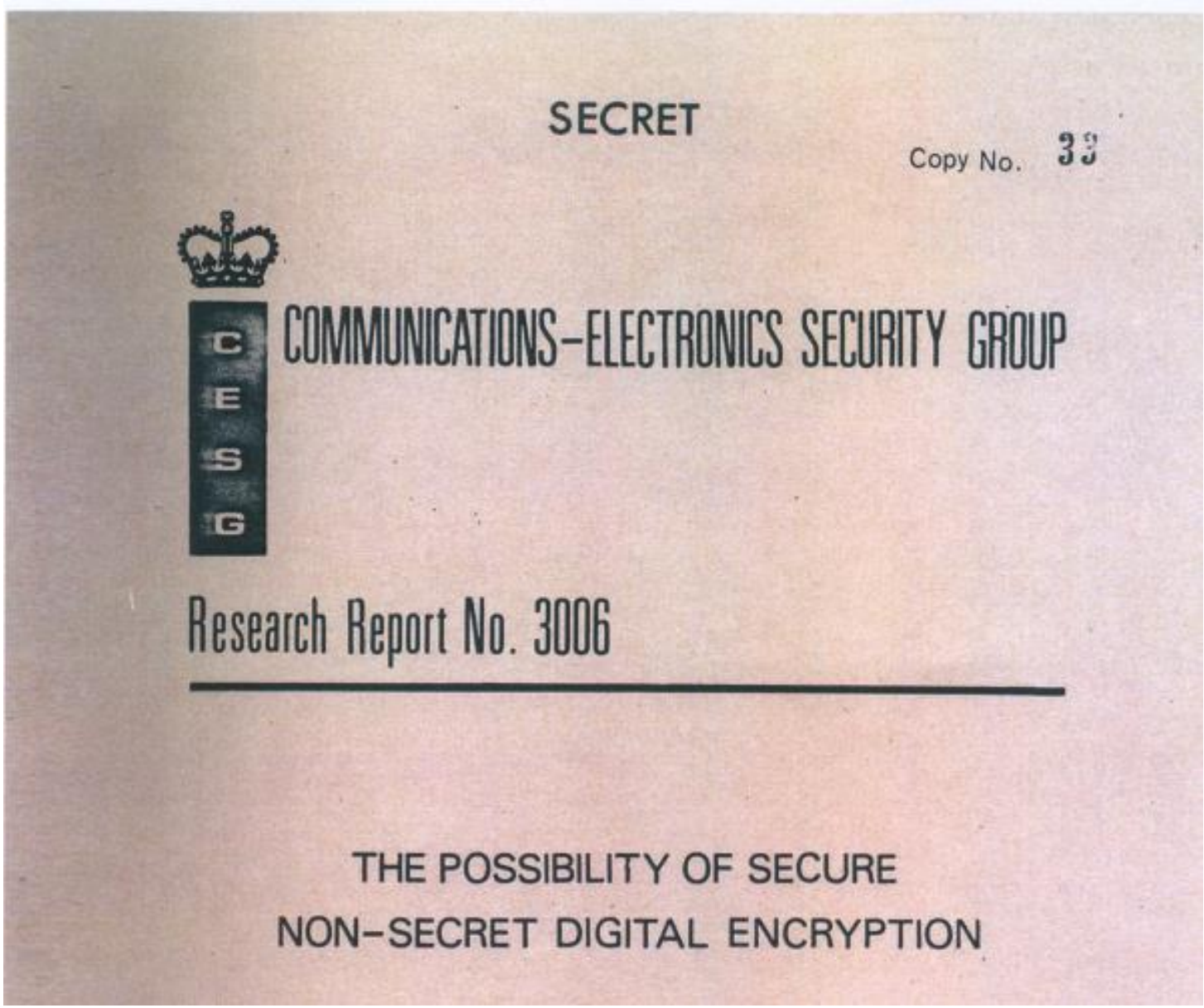


Ron Rivest, Adi Shamir and Leonard Adleman (1977)

10 years earlier (at GCHQ)…

James Ellis

Clifford Cocks



SECRET

Copy No. 33

COMMUNICATIONS-ELECTRONICS SECURITY GROUP

C E S G

Research Report No. 3006

THE POSSIBILITY OF SECURE
NON-SECRET DIGITAL ENCRYPTION

Summary

This report considers the problem of achieving secure transmission of digital information in the circumstances where there is no information initially possessed in common by the two legitimate communicators which is not also known to the interceptor. It demonstrates, by means of a model having the required properties that a theoretical solution exists, but does not establish that a practical system can be devised.

Case No. 305 refers

Date of approval for issue:
January 1970

THE POSSIBILITY OF SECURE NON-SECRET
DIGITAL ENCRYPTION"
THEORETICAL SYSTEM

Z32491
SECRET

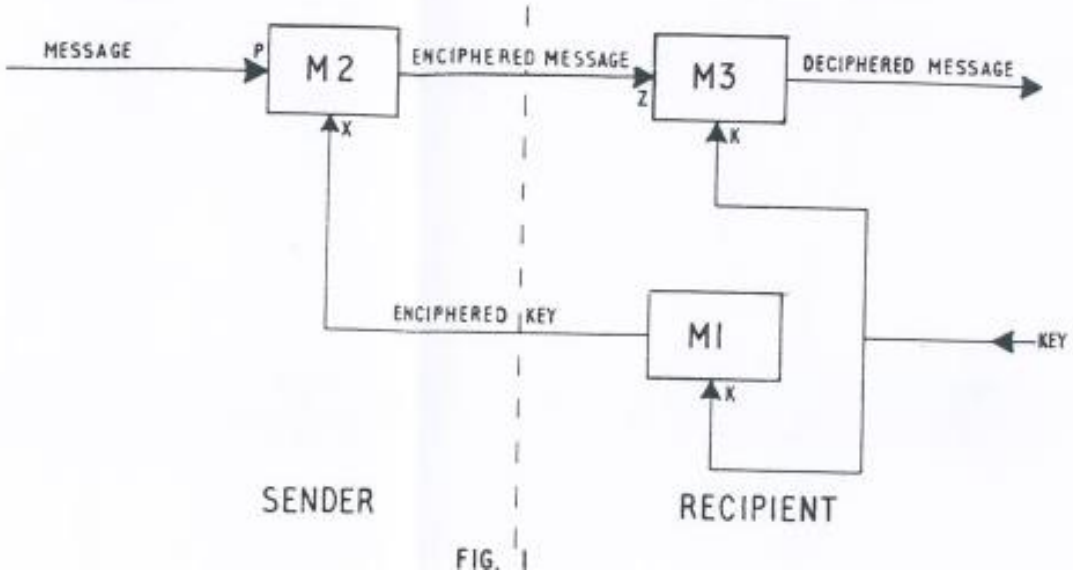


FIG. 1

SECRET

RSA Recipe

- Public Key n=1457 and e=809 (I chose these)
- To encrypt a message, M, $1<M<1457$ you compute $C=M^e \bmod 1457$
- You tell me C
- I can then work out M

What am I doing?

- Public Key n=1457 and e=809
- You chose M and told me $C=M^e \bmod 1457$
- I compute $C^{29} \bmod 1457$ to recover M
- This works because for any choice of M

$$M^{809\times 29}=M \bmod 1457$$

- Why?

Fermat's Little Theorem

- Let p be a prime and a an integer that is not a multiple of p (so a and p are relatively prime).
- Then

$$a^{p-1}=1 \bmod p$$

Euler's Theorem

- Let n and a be relatively prime, then

$$a^{\varphi(n)}=1 \bmod n$$

where $\varphi(n)$ counts the numbers from 1 to n that are relatively prime to n (e.g. $\varphi(p)=p-1$).

The numbers relatively prime to *n* form a group under multiplication mod *n*

$\acute{}_{15}$	1	2	4	7	8	11	13	14
1								
2								
4								
7								
8								
11								
13								
14								

The numbers rel. prime to *n* form a group under multiplication mod *n* of order φ(*n*)

´ 15	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Fermat's Little Theorem

- Let p be a prime and a an integer that is not a multiple of p (so a and p are relatively prime).
- Then

$$a^{p-1}=1 \bmod p$$

Euler's Theorem

- Let n and a be relatively prime, then

$$a^{\varphi(n)}=1 \bmod n$$

where $\varphi(n)$ counts the numbers from 1 to n that are relatively prime to n (e.g. $\varphi(p)=p-1$).

More generally

- Choose primes p,q and work out $n=p\times q$
- Compute $\varphi(n)=(p-1)(q-1)$
- Choose e relatively prime to $\varphi(n)=(p-1)(q-1)$
- Typically $e=65{,}537=2^{16}+1$
- Work out $d=e^{-1} \bmod \varphi(n)$
- Public Key n and e
- To encrypt a message M compute $C=M^e \bmod n$
- The receiver computes C^d to recover M
- How secure is this?

More generally

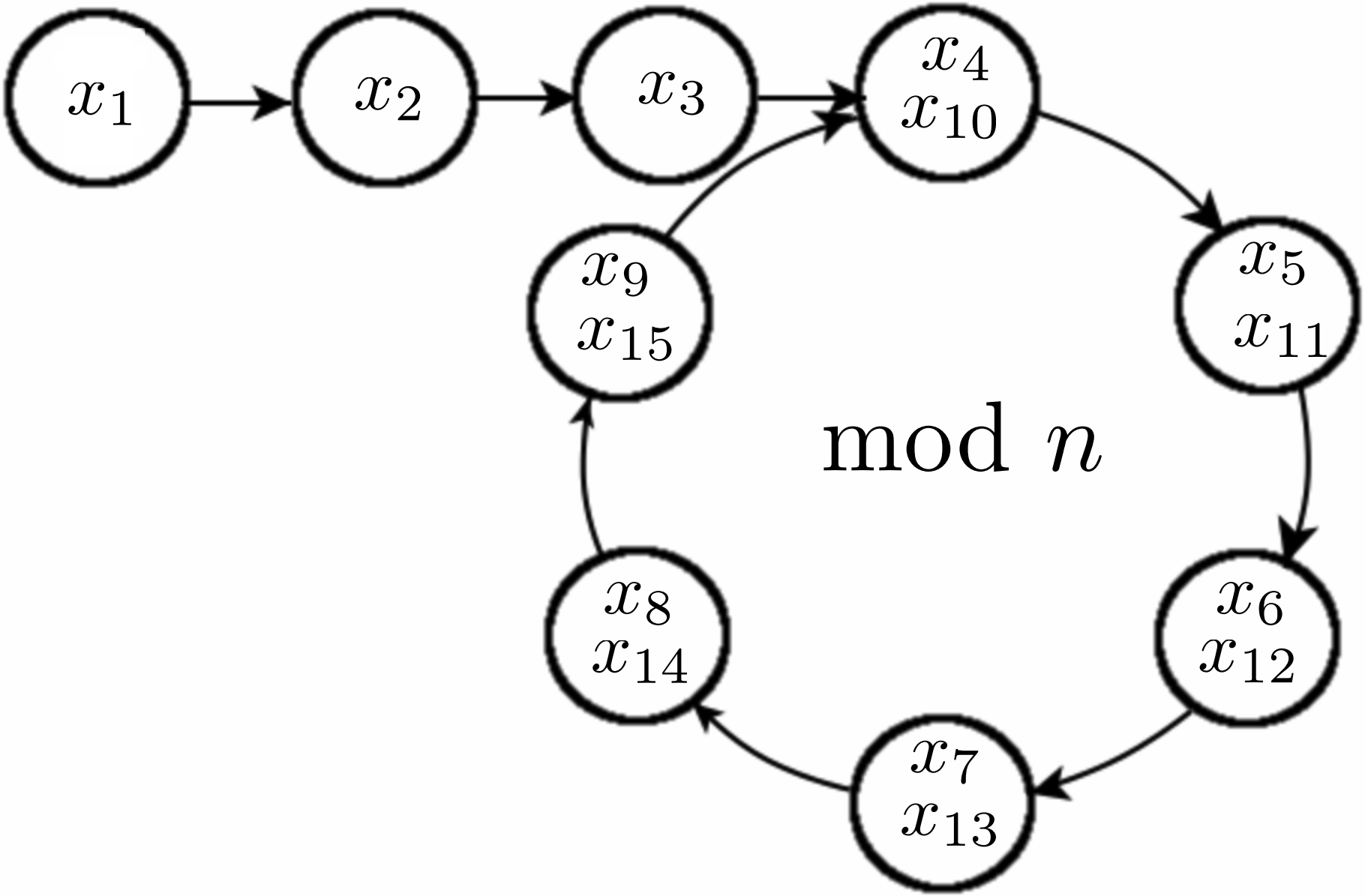
- Choose primes p,q and work out $n=p\times q$
- Compute $\varphi(n)=(p-1)(q-1)$
- Choose e relatively prime to $\varphi(n)=(p-1)(q-1)$
- Typically $e=65{,}537=2^{16}+1$
- Work out $d=e^{-1} \bmod \varphi(n)$
- Public Key n and e
- To encrypt a message M compute $C=M^e \bmod n$
- The receiver computes C^d to recover M
- How secure is this?

The following is a product of two primes

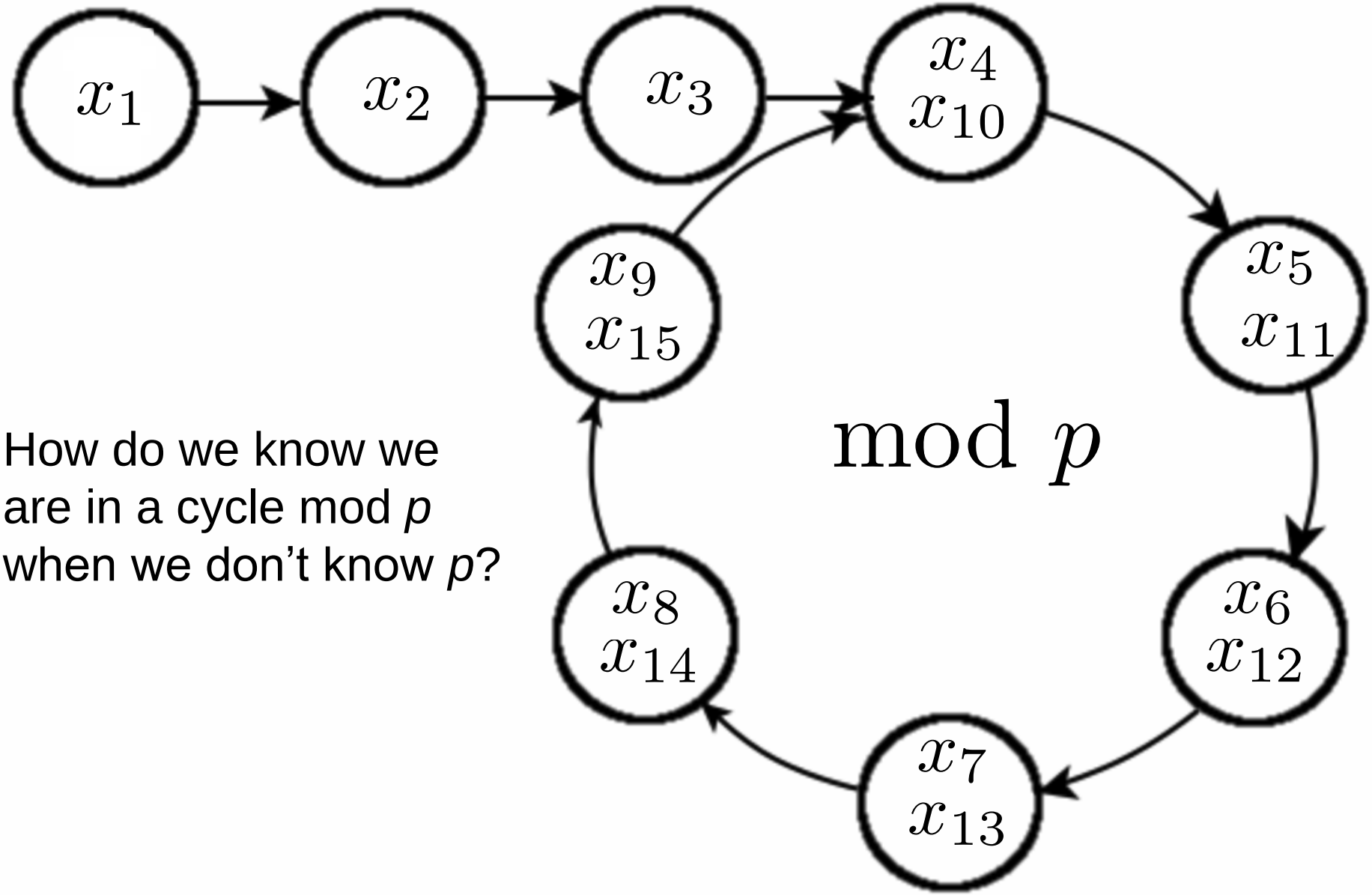
- 25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249415082189298559149176184502808489120072844992687392807287776635971141834727026189637801497824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654612282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544541784240209246165157233507787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103971228221207203 57
- How can we find them?

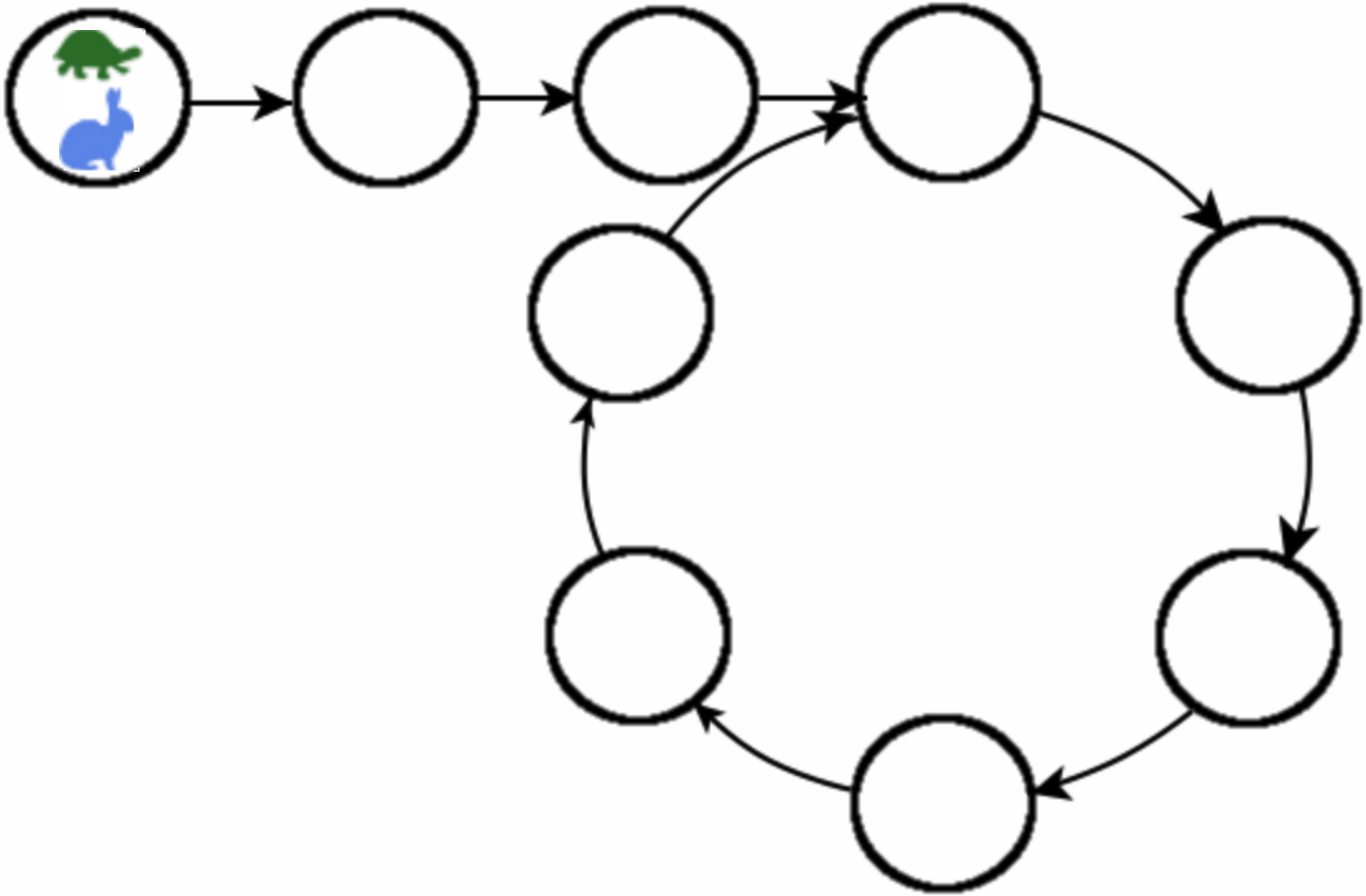
$n=p\times q$, we know n but not p or q

- Choose a polynomial, e.g. $f(x)=x^2+1$
- Choose $x_1=a$ and define $x_{k+1}=f(x_k) \bmod n$
- The sequence $x_1, x_2, x_3,\ldots$ eventually repeats
- We can see this happening because we know n


x_1
x_2
x_3
x_4
x_{10}
x_5
x_{11}
x_6
x_{12}
x_7
x_{13}
x_8
x_{14}
x_9
x_{15}
mod n

How do we know we are in a cycle mod *p* when we don't know *p*?





Pollard's Rho Algorithm

- Take n (a product of unknown primes p and q)
- Choose a polynomial, e.g. $f(x)=x^2+1$
- Choose $x_1=a$ and define $x_{k+1}=f(x_k) \bmod n$
- Check $\text{hcf}(|x_2 - x_1|, n)$
- Check $\text{hcf}(|x_4 - x_2|, n)$
- Check $\text{hcf}(|x_6 - x_3|, n)$
- Check $\text{hcf}(|x_8 - x_4|, n)$…

Most will have hcf=1 but eventually x_{2k} and x_k will be equal modulo p and then $\text{hcf}(|x_{2k} - x_k|, n) = p$ (usually).