Everything you always wanted to know about cryptography but were afraid to ask…

Lord egeltje

Content

- What is cryptography?
- Classical ciphers
- Modern ciphers
  - Stream ciphers
  - Block ciphers
    - Symmetric (DES, AES)
    - Asymmetric (RSA, ECC)
- Future ciphers
  - Post-quantum cryptography

- Disclaimer: some extremely complicated stuff is simplified to be more readable.

What is cryptography?

What is cryptography?

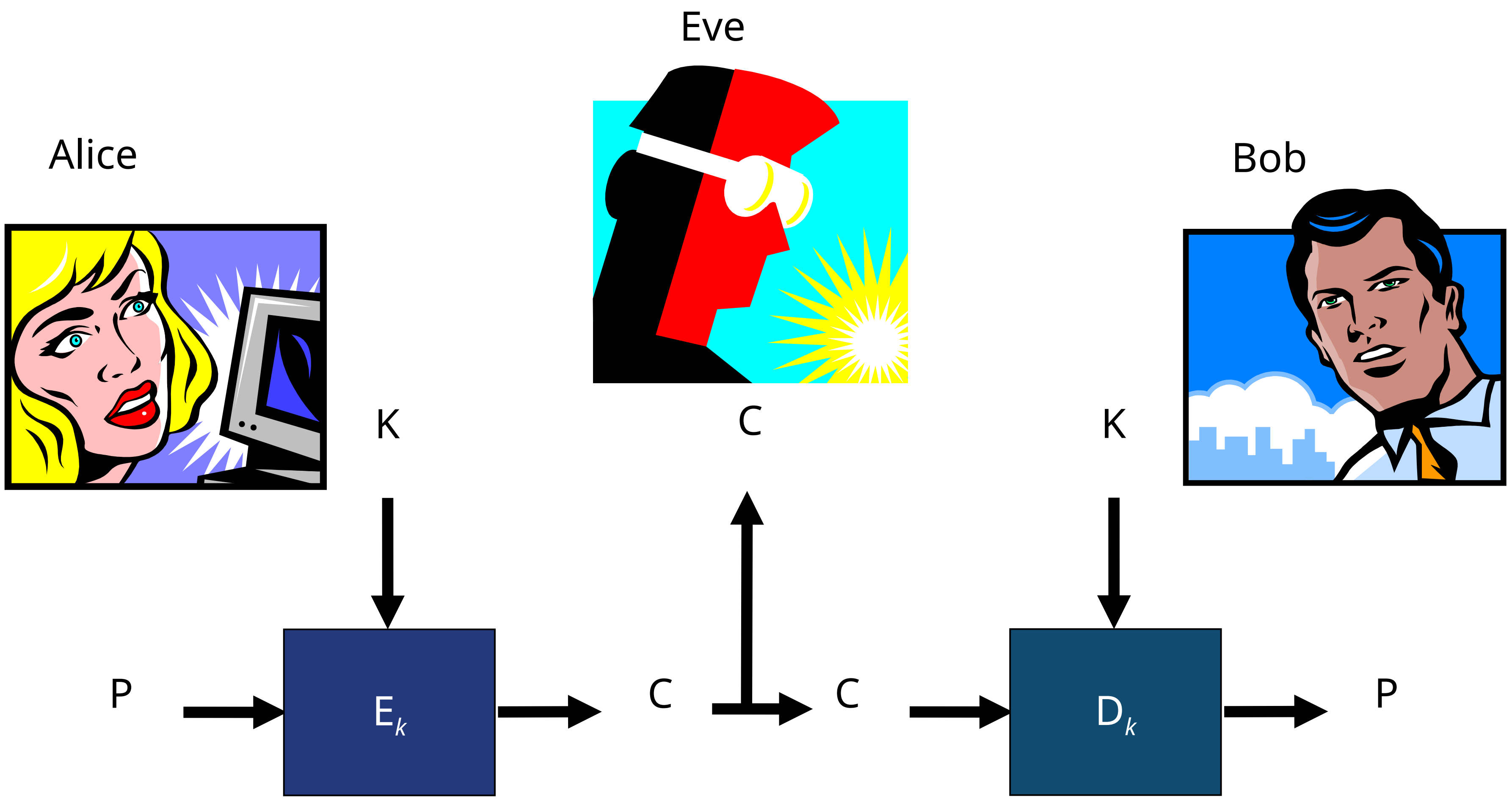
- Cryptography is used to scramble a message and allow descrambling if a few (secret) facts are known on the scrambling method (so no base64!)

- Words I'll be using a lot:

• Plain text	original message
• Key	codeword used for encryption
• Cipher	algorithm used for encryption or crypto system
• Cipher text	encrypted message

- Cryptology
  - Cryptography (design ciphers)
  - Cryptanalysis (break ciphers)

A typical scenario



Classical ciphers

Classical ciphers

- Cryptography is from all ages and can have many forms

- This is a very secret message
- Τηισ ισ α ϖερψ σεχρετ μεσσαγε

Classical ciphers – mono-alphabet substitution

- Replace the character by another character (of the same alphabet).

- Number of possible keys = 26! ($26 \cdot 25 \cdot 24 \cdot \ldots \cdot 1$).
- Number of useful keys much lower.

- Language statistical properties fully present:
- Most occuring characters in english are the e, t, a, o, n, I.
- Certain characters often appear together (“the”, “qu”).

Classical ciphers – mono-alphabet substitution

- Caesar cipher
- Shift the alphabet by a number of *n* characters.
- If plain text and cypher are known, the key can be deduced (even with one character).
- Number of possible keys?

Classical ciphers – mono-alphabet substitution

- Caesar cipher

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
m n o p q r s t u v w x y z a b c d e f g h i j k l
```

n = 13 (aka: rot13)

```
Meet me after the toga party
Yqqf yq mrfqd ftq fasm bmdfk
```

Classical ciphers – mono-alphabet substitution

- Caesar cipher - A small test

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
d e f g h i j k l m n o p q r s t u v w x y z a b c
```

n = 3 (actual number used by Julius Caesar)

```
attack the castle at dawn
dwwdfn wkh fdvwoh dw gdzq
```

Classical ciphers – poly-alphabet substitution

- First described by monk Trittenheim in 1518
- Use alphabet matrix to mix plain text with key
- Language statistical properties hardly present (different shifts are used for different characters, shift is determined by key character)
- If plain text and cipher are known, the key can be deduced

Classical ciphers – poly-alphabet substitution

- Vigenére cipher

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
b c d e f g h i j k l m n o p q r s t u v w x y z a
c d e f g h i j k l m n o p q r s t u v w x y z a b
d e f g h i j k l m n o p q r s t u v w . . . . . .
e f g . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . t u v
. . . . . . d e f g h i j k l m n o p q r s t u v w
y z a b c d e f g h i j k l m n o p q r s t u v w x
z a b c d e f g h i j k l m n o p q r s t u v w x y
```

Classical ciphers – poly-alphabet substitution

- Vigenére cipher

`attack the castle at dawn`	`plain text`
`secret sec retsec re tsec`	`key`
`sxvrgd llg tellpg rx wsap`	`cipher`

C = ((P + K) – 1) mod 26 and P = ((C – K) + 1) mod 26

K = ((C – P) + 1) mod 26

Classical ciphers – Enigma

- Mythical device…
- Invention atributed to Van Hengel and Sprengler in 1915
- Started commercial, addopted by Germans in WWII
- Poly-alphabet substitution
- Cryptanalysis by Polish mathematicians, improved by British cryptographers
- Brute force via Bombe with known plain text (“crib”)

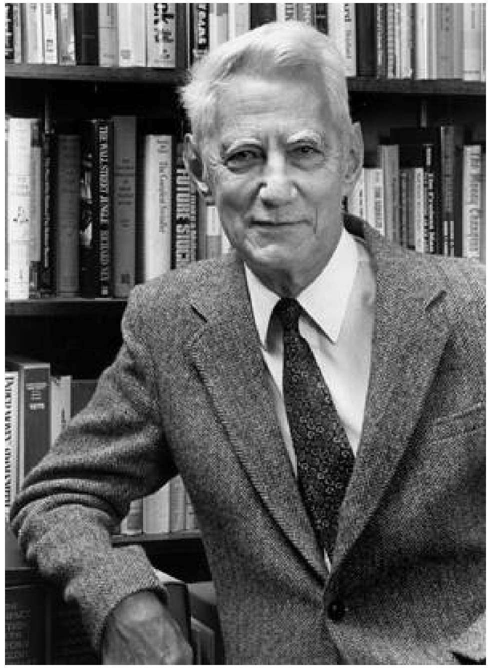
Modern ciphers

Modern ciphers

- Huge demand for faster algorithms

- Claude Shannon wrote some of the pivotal papers on modern cryptology theory in 1949
  - Communication Theory of Secrecy Systems
  - Prediction and Entropy of printed English

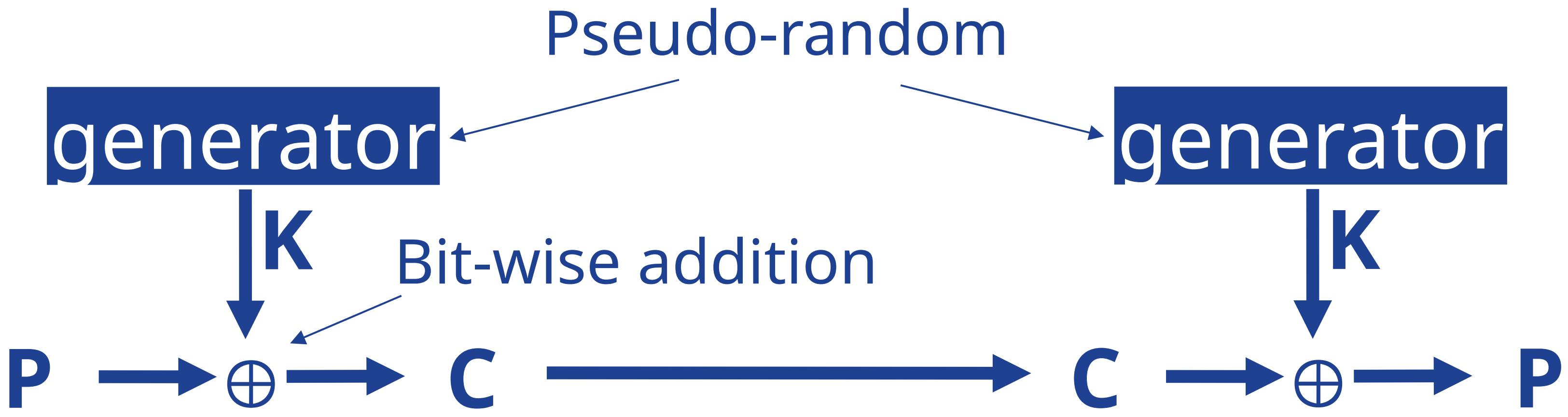
- In these he developed the concepts of
  - entropy of a message
  - redundancy in a language
  - theories about how much information is needed to break a cipher1
  - defined concepts of computationally secure vs unconditionally secure



Modern ciphers – stream ciphers

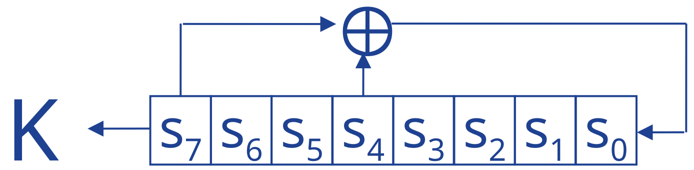
- Stream of characters encrypted, such that the encryption is not the same for each character in the stream (“memory” effect).

- Useful for
  - real-time data transmission
  - unpredictable amount of characters.



Modern ciphers – stream ciphers – algorithms

- Generator is often Linear Feedback Shift Register (LFSR)
- Key output depending on previous key output, not on message



$$f_{(x)} = x^7 + x^4 + x^0$$

Modern ciphers – stream ciphers – algorithms

- GSM (A5)
- Bluetooth
- Wifi (WEP)

- Mifare classic (Crypto1)

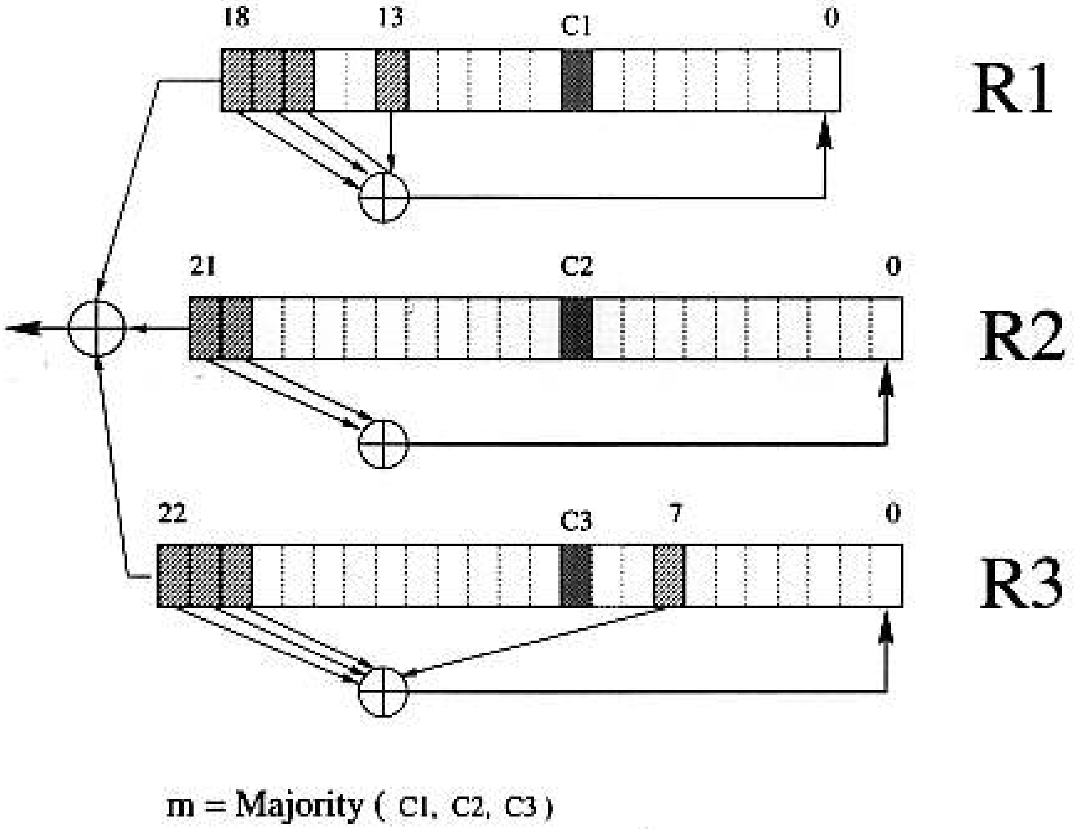
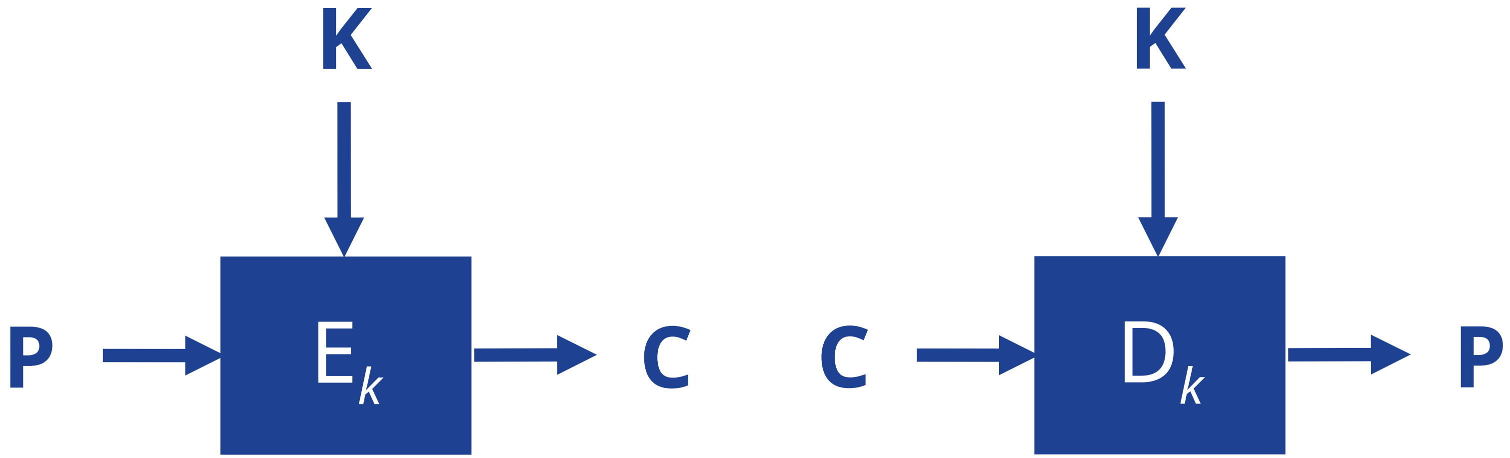


Figure 1: The A5/1 stream cipher.

Modern ciphers – block ciphers

- Blocks of characters are encrypted



Modern ciphers – block ciphers

- Symmetric (both sides have the same key)
  - Useful for large amounts of text
  - Requires a lot of relatively simpel computations (can easily be implemented in hardware)
  - Limitation that the key must already be known by the sender and receiver

- Asymmetric (both sides have different but related keys)
  - Useful for symmetric key exchange
  - Useful for identity proof
  - Requires a lot of complex computations
  - Limitation that the message m_a must be smaller than the n_b

Modern ciphers – symmetric block ciphers - DES

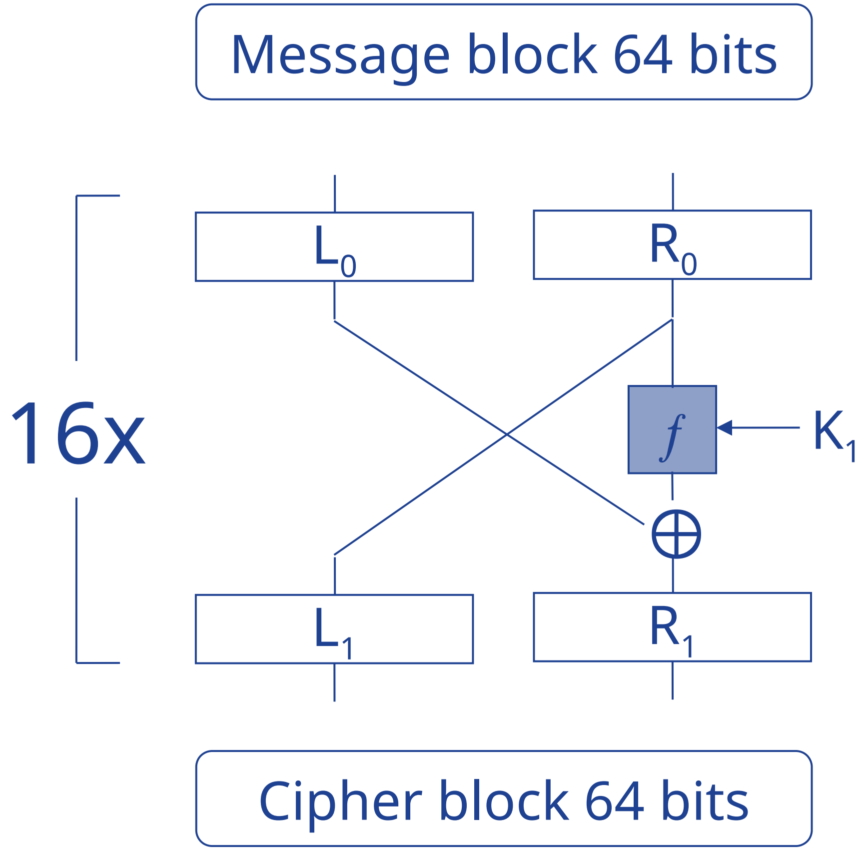
- Data Encryption Standard

- Originally proposed by IBM in 1974 to call by NBS (with 112 bits key)
- Derived from IBM's "LUCIFER" (Horst Feistel, Walter Tuchman)

- US Export restrictions
- Criticism by Diffie & Hellman in 1975: Key too short (only 56 bits in DES)

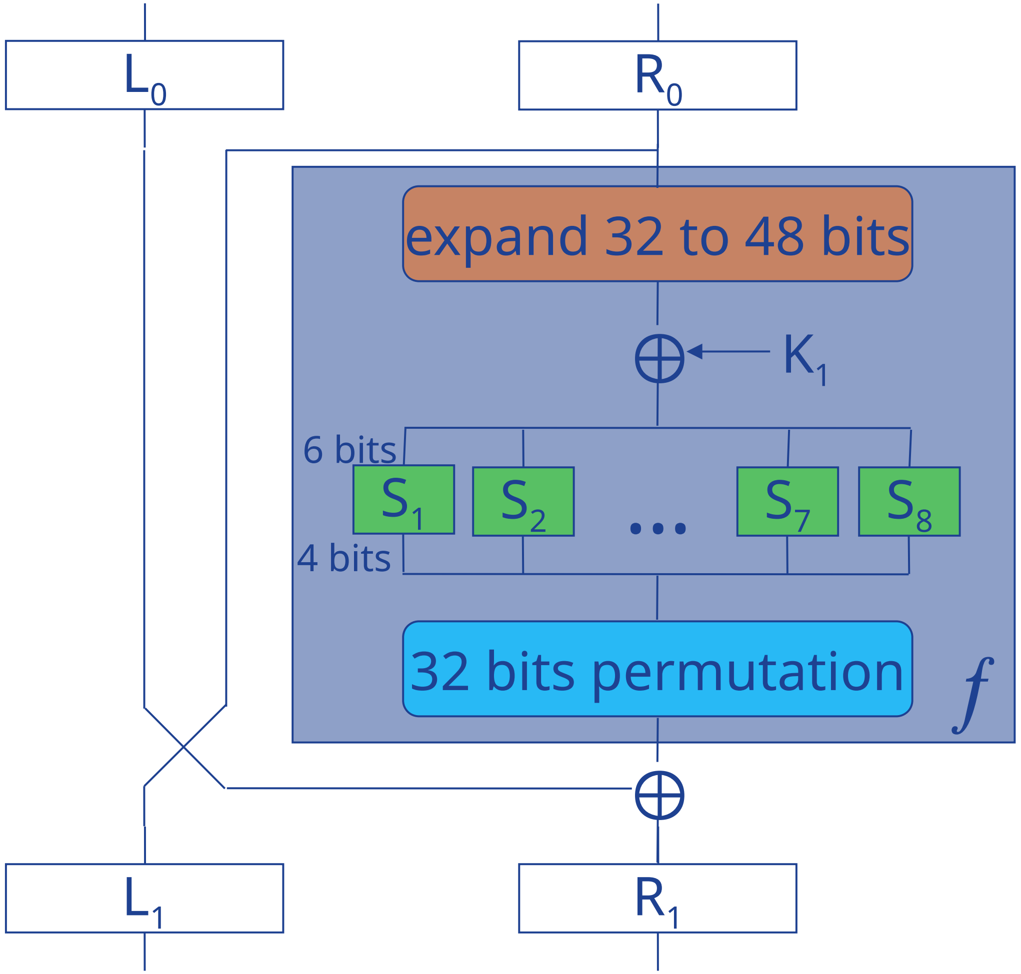
Modern ciphers – symmetric block ciphers - DES

- Feistel cipher
- L_x and R_x 32 bits
- K_x 48 bits round key derived from 56 bits key



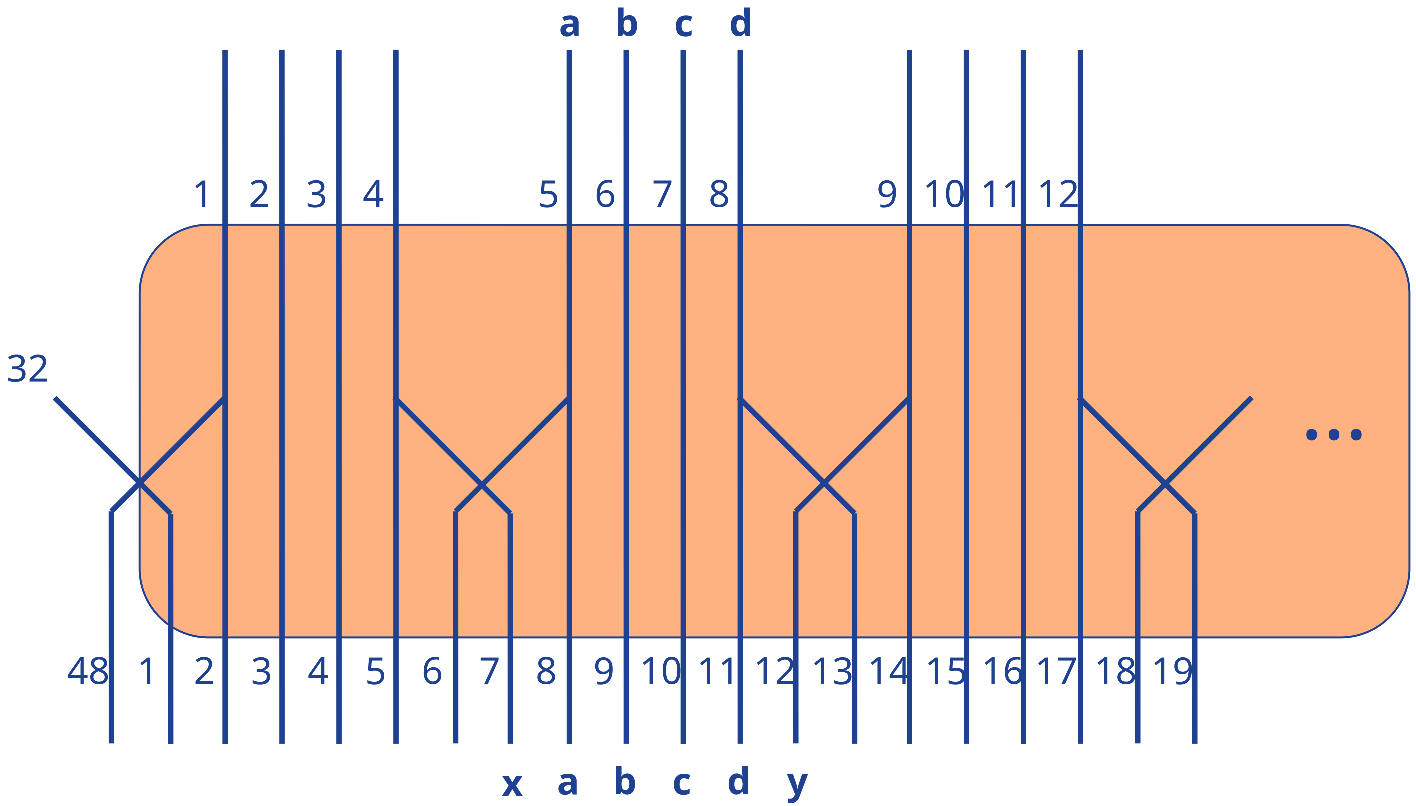
Modern ciphers – symmetric block ciphers - DES

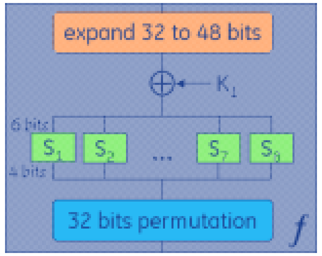
- Expand 32 bits to 48 bits
- Add 48 bits round key
- Through S-boxes
- Permutation (shuffle)



Modern ciphers – symmetric block ciphers - DES

- Expand 32 bits to 48 bits





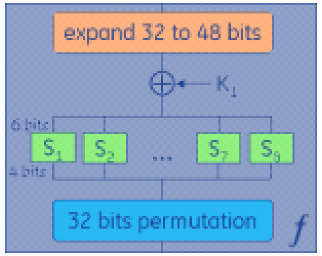
Modern ciphers – symmetric block ciphers - DES

- S-Boxes (substitution)
- Content carefully chosen!
- Changing one input bit results in changing of approximately half the output bits
- NSA controversy

abcd

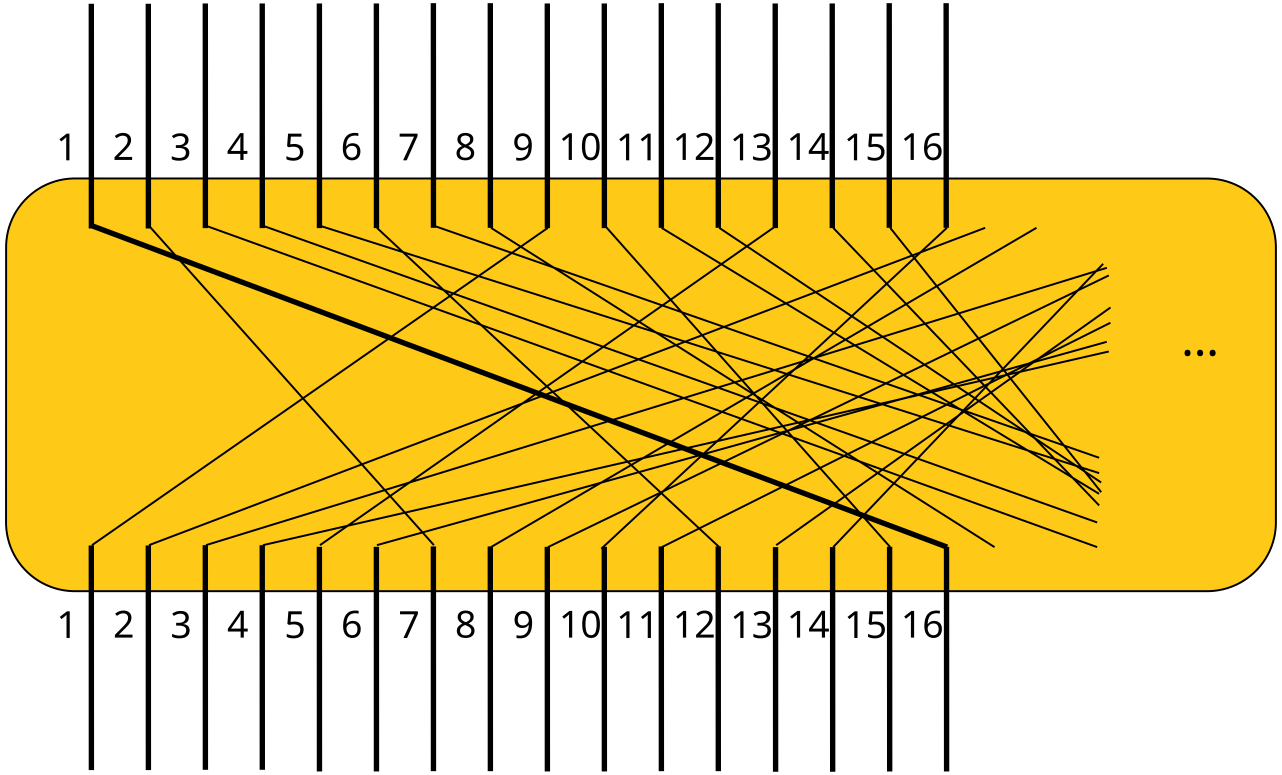
xy

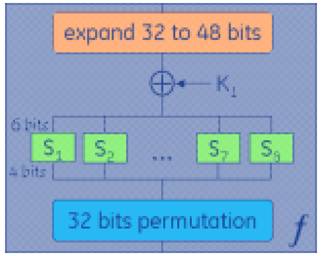
S1	00	01	10	11
0000	**14**	**00**	**04**	**15**
0001	**04**	**15**	**01**	**12**
0010	**13**	**07**	**14**	**08**
0011	**01**	**04**	**08**	**02**
0100	**02**	**14**	**13**	**04**
0101	**15**	**02**	**06**	**09**
0110	**11**	**13**	**02**	**01**
0111	**08**	**01**	**11**	**07**
1000	**03**	**10**	**15**	**05**
1001	**10**	**06**	**12**	**11**
1010	**06**	**12**	**09**	**03**
1011	**12**	**11**	**07**	**14**
1100	**05**	**09**	**03**	**10**
1101	**09**	**05**	**10**	**00**
1110	**00**	**03**	**05**	**06**
1111	**07**	**08**	**00**	**13**



Modern ciphers – symmetric block ciphers - DES

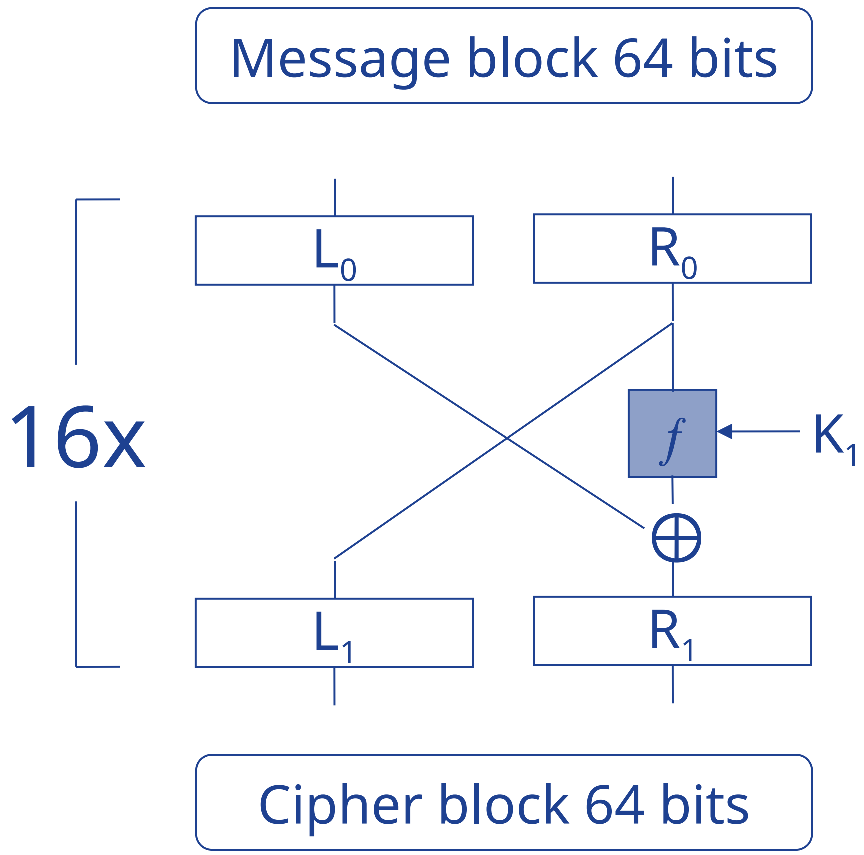
- P-boxes (permutation)





Modern ciphers – symmetric block ciphers - DES

- Feistel cipher

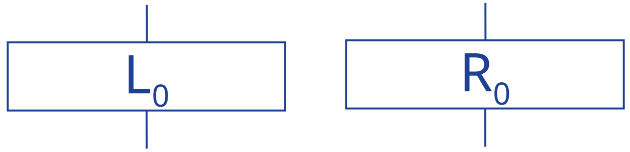


Modern ciphers – symmetric block ciphers - AES

- Call by NIST in 1997
- DES over 20 years old
- Key of 56 bits does not offer an acceptable level of security for some applications
- 3DES relatively slow
- Winning algorithm RIJNDAEL (V. Rijmen, J. Daemen (B))
- 128, 192 or 256 bits key

Modern ciphers – symmetric block ciphers - AES

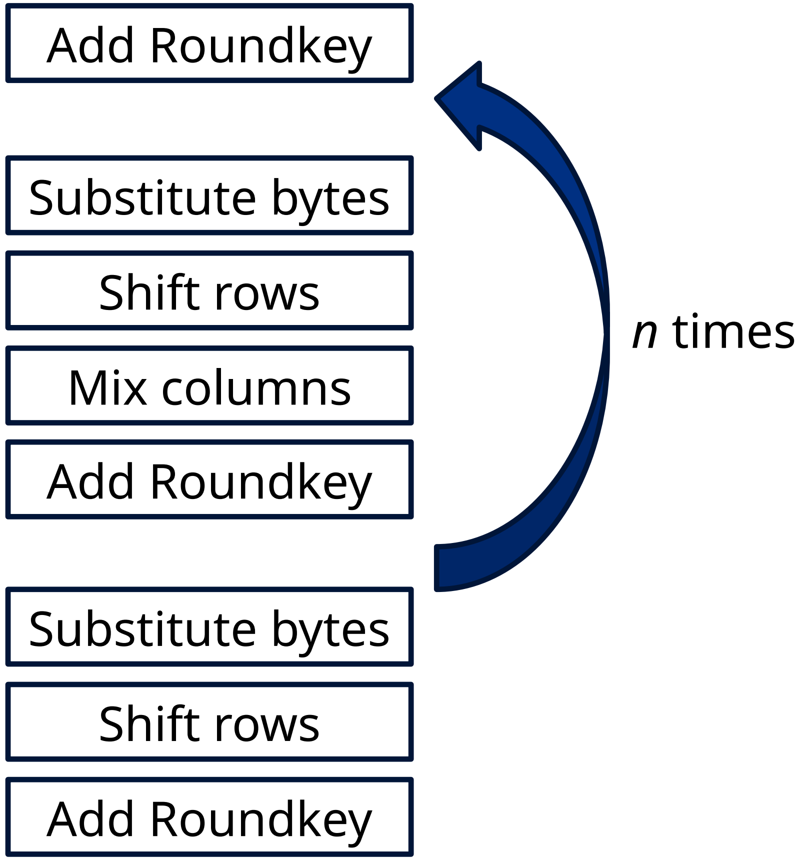
- DES uses 64 consequetive bits



- AES uses a 4 x 4 byte matrix

D_0	D_1	D_2	D_3
D_4	D_5	D_6	D_7
D_8	D_9	D_{10}	D_{11}
D_{12}	D_{13}	D_{14}	D_{15}

Modern ciphers – symmetric block ciphers - AES

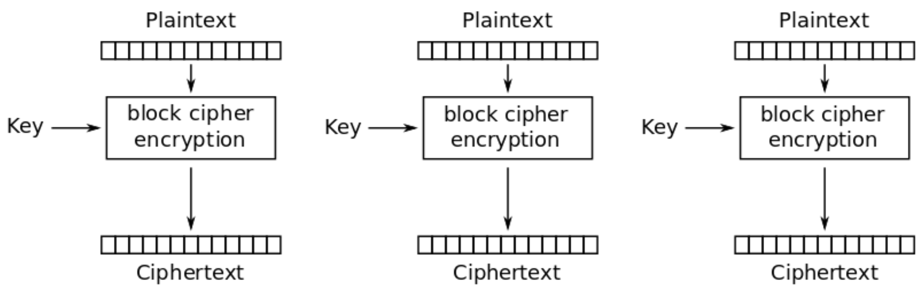


D_0	D_1	D_2	D_3
D_4	D_5	D_6	D_7
D_8	D_9	D_{10}	D_{11}
D_{12}	D_{13}	D_{14}	D_{15}

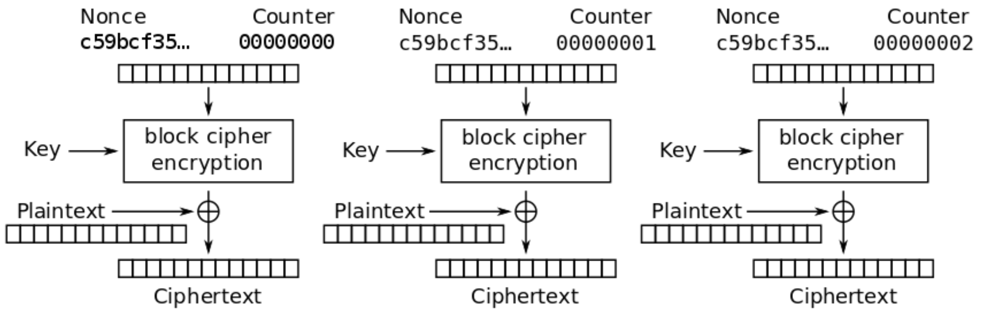
- AES128 n = 10
- AES192 n = 12
- AES256 n = 14

Modern ciphers – symmetric block ciphers - modes

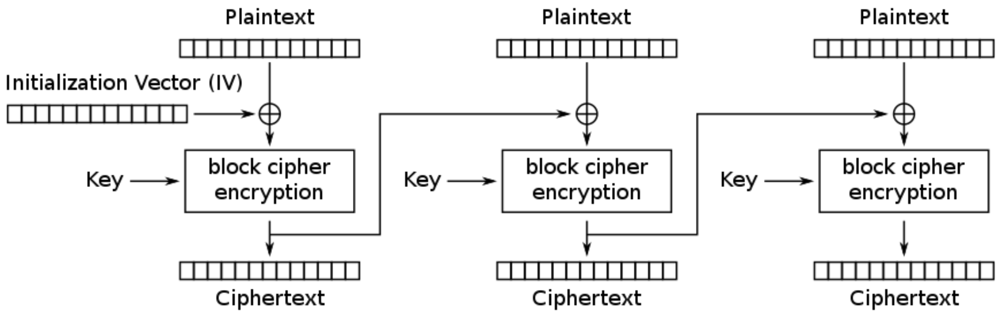
- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Counter Mode (CTR / xCM)



Electronic Codebook (ECB) mode encryption

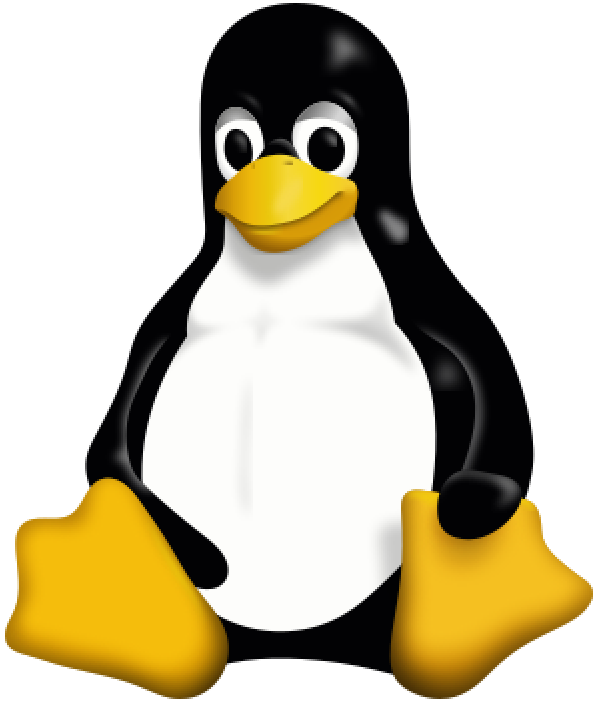


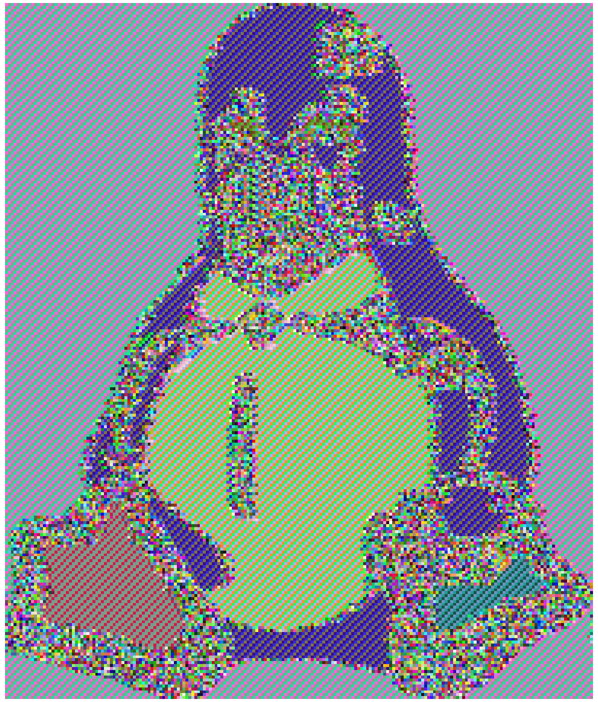
Counter (CTR) mode encryption

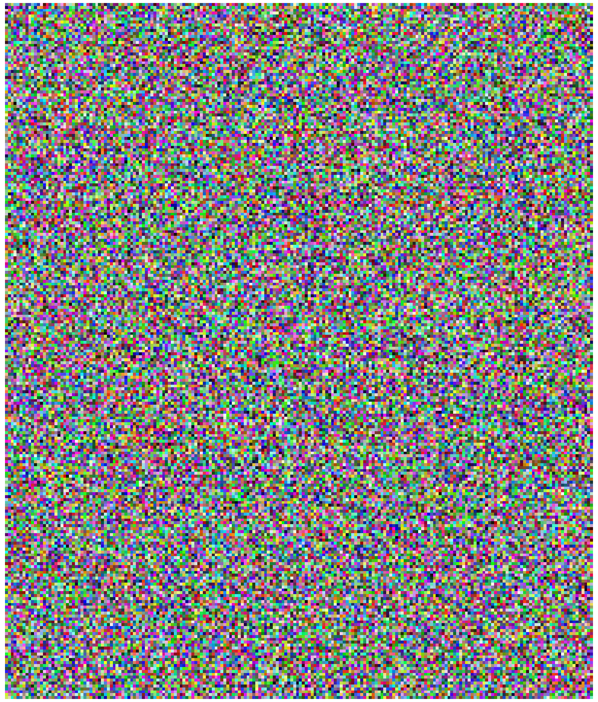


Cipher Block Chaining (CBC) mode encryption

Modern ciphers – symmetric block ciphers - modes







Modern ciphers – keys

- As we saw with Vigenére, a common word (or sentence) has to be known by both parties (sender and receiver).

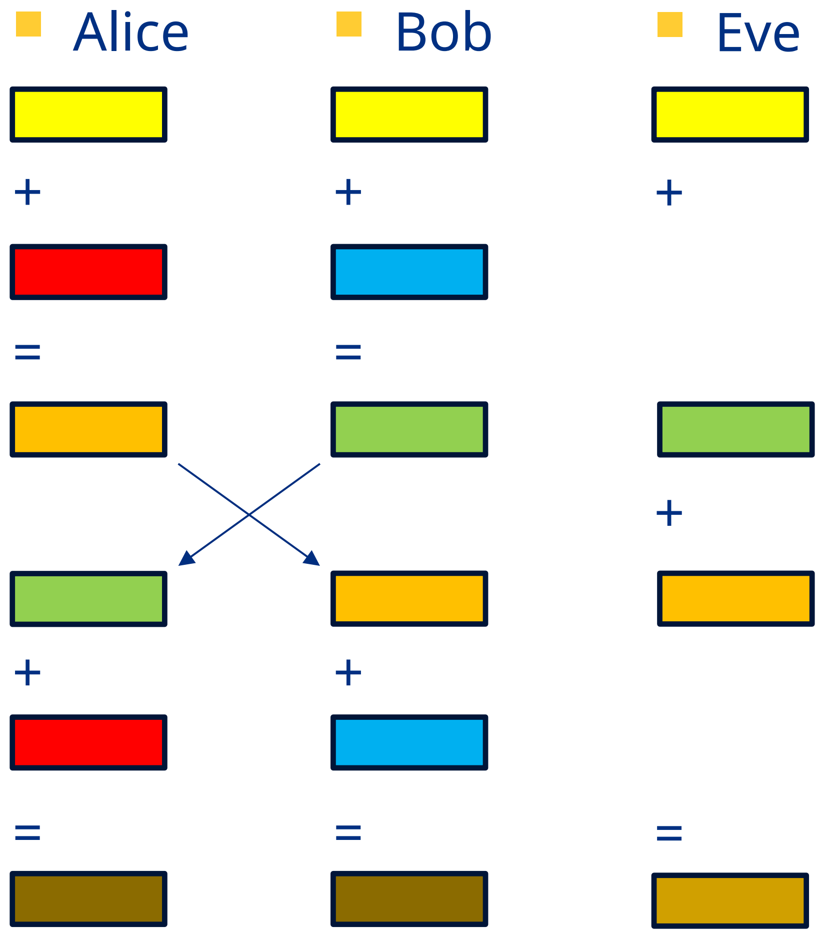
- If plain text, cipher text and algorithm are known, the key should not* be deducible. (Kerckhoffs' Principle, 1883).

- Symmetric keys: $K_e = K_d$
- Asymmetric keys: $K_e \neq K_d$ and K_d not deducible from K_e

* Or at least computational infeasible

Modern ciphers – key exchange (Diffie – Hellman)

- Common
- Add secret
- Result
- Add secret
- Result



Lame claim to fame: I had dinner with Whit Diffie (and Bruce Schneier and David Kahn and Jos Weyers) at Bletchley Park

Modern ciphers – asymmetric ciphers - RSA

- Published by Ron Rivest, Adi Shamir, Leonard Aldeman in 1977
- GCHQ's Clifford Cook was first in 1973, but it was classified
- Relies on the computationally intensive factoring of large prime numbers
- Easy to calculate $(p - 1) \cdot (q - 1) = \varphi$
- Hard to find $\varphi = (?? - 1) \cdot (?? - 1)$

Modern ciphers – demo RSA
10 seconds of math – Greatest Common Divisor (GCD)

- Greatest Common Divisor is the greatest number that divides two numbers.
- GCD(8, 18) = 2
- GCD(24, 36) = 12
- GCD(21, 36) = 3
- GCD(21, 41) = 1 (because 41 is a prime number)

Modern ciphers – demo RSA
10 seconds math – modulus

- Substracting *k* times a number *p* from another number *a* as long as a number is positive, which leaves a remainder *r*. *k* is not important.

$$a = r + k \cdot p \equiv a = r \bmod(p)$$

- 118 = 58 mod(60) 118 seconds = 1 minute + 58 sec.
- 15 = 1 mod(7) 15 days = 2 weeks + 1 day
- 12345678901234567890 = 0 mod (10)
- 264 = 18 mod(34)

Modern ciphers – demo RSA
10 seconds math – Theorems of Fermat and Euler

- Take for a and p relative prime numbers so GCD(a, p) = 1 and $1 < a < p$, then:

Fermat: $a^{p-1} = 1 \bmod(p)$

Euler: $a^{\varphi(p)} = 1 \bmod(p)$

$\varphi(p)$ = all positive numbers smaller than p that are relative prime with p

if p is prime, then $\varphi(p) = p - 1$

Modern ciphers – demo RSA
Key setup

- Bob choses 2 primes p_b and q_b and calculates the products

  $$p_b \cdot q_b = n_b \quad \text{and} \quad \varphi(n_b) = (p_b - 1) \cdot (q_b - 1)$$

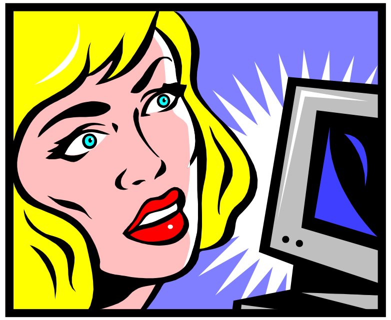
- Bob choses encryption exponent e that is relative prime to $\varphi(n_b)$

- Bob calculates decryption exponent d_b so $e_b \cdot d_b = 1 \bmod(\varphi(n_b))$

- Bob publishes e_b and n_b , keeps d_b secret

Modern ciphers – demo RSA
Message encryption

- Alice has a secret message m_a,
- calculates $(m_a)e_b = c_a \bmod(n_b)$
- and passes c_a to Bob



Modern ciphers – demo RSA
Message decryption

- Bob receives c_a,
- calculates $(m_a)d_b = m_a \bmod(n_b)$
- and finds m_a

Proof:

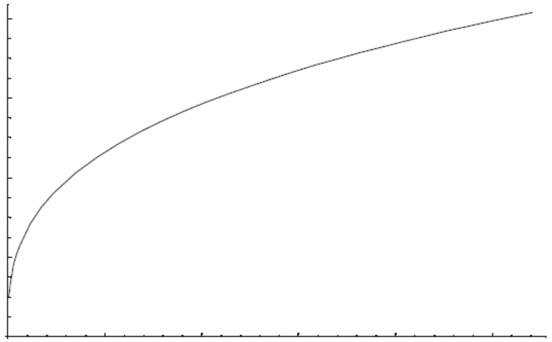
$$((m_a)^{e_b})^{d_b} \equiv (m_a)^{e_b \cdot d_b} \equiv (m_a)^{1 mod(\varphi(n_b))} \equiv (m_a)^{1 + k \cdot \varphi(n_b)}$$
$$\equiv m_a \cdot (m_a)^{k \cdot \varphi(n_b)} \equiv m_a \cdot ((m_a)^{\varphi(n_b)})^k \equiv m_a \cdot (1)^k$$
$$\equiv m_a \bmod(n_b)$$

Modern ciphers – demo RSA Cryptanalysis

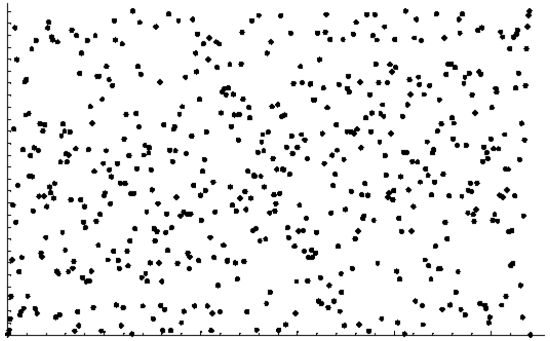
- Eve receives c_a and has knowledge of n_b and e_b
- Eve has to solve $(??)^{e_b} = c_a \bmod (n_b)$
- Take the e_b–th modular root of c_a

Modern ciphers – demo RSA Cryptanalysis

- Take the e_b–th root of c_a



- Take the e_b–th modular root of c_a

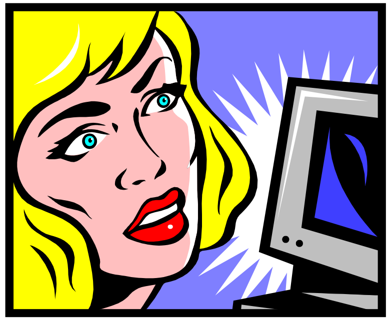


Modern ciphers – demo RSA
Key setup

- p_b = 17
- q_b = 37
- n_b = $p_b \cdot q_b$ = 629
- $\varphi(n_b)$ = $(p_b - 1) \cdot (q_b - 1) = (17 - 1) \cdot (37 - 1) = 576$
- e_b = 41, GCD(eb, φ(nb)) = 1, $1 < e_b < \varphi(n_b)$
- d_b = 281, (because $41 \cdot 281 = 1 \bmod(576)$)

Modern ciphers – demo RSA
Message encryption

- m_a = 55, this is the plain text
- n_b = 629
- e_b = 41
- Calculate $55^{41} = 89 \bmod(629)$
- Send “89” to Bob



Modern ciphers – demo RSA
Message decryption

- m_a = 89, this is the cipher
- n_b = 629
- d_b = 281
- Calculate $89^{281} = 55 \bmod(629)$
- 55 was the secret message of Alice

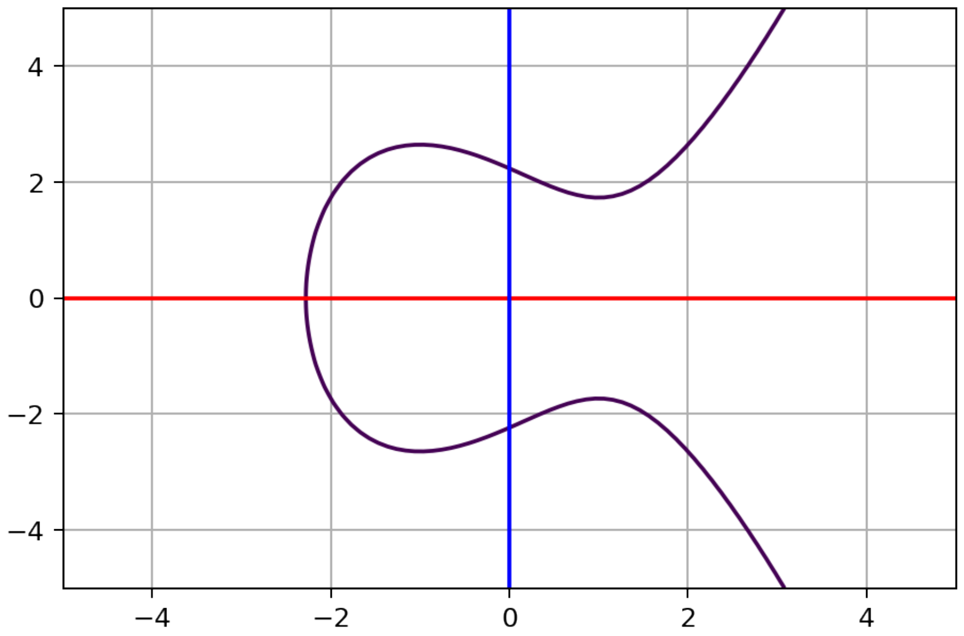
Modern ciphers – demo RSA Cryptanalysis

- c_a = 89
- n_b = 629
- e_b = 41
- Calculate $??^{41} = 89 \bmod(629)$

Modern ciphers – asymmetric ciphers - ECC

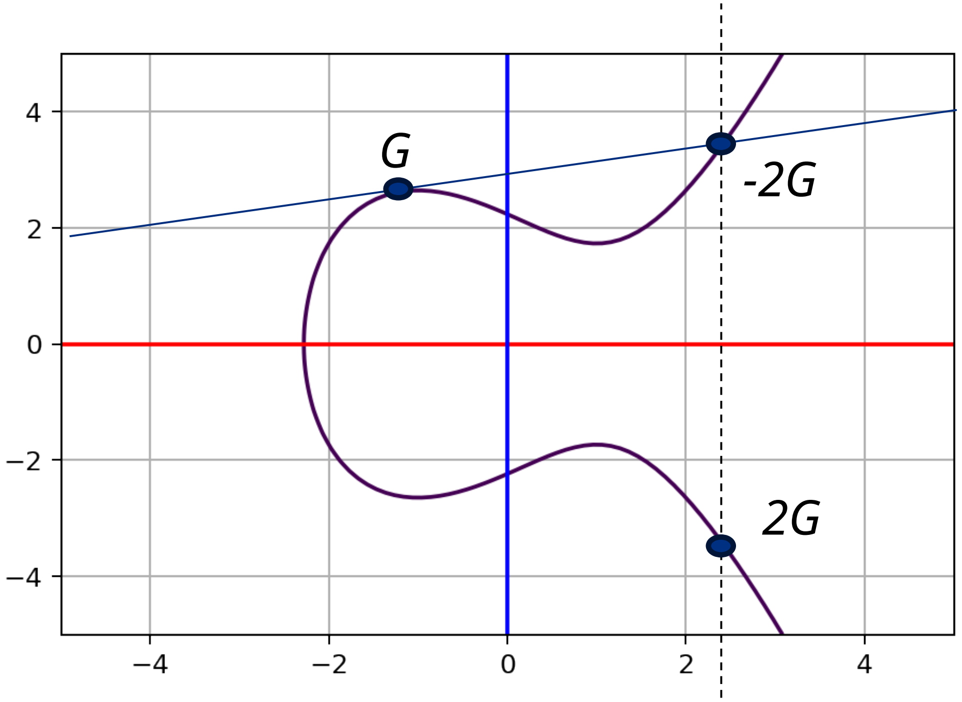
- Walk around a “Weierstrass” curve of the shape $y^2 = x^3 + ax + b$ to reach a point (to be more precise $(y^2 - x^3 - ax) \bmod p = 0$, where p is the prime generating a finite field)

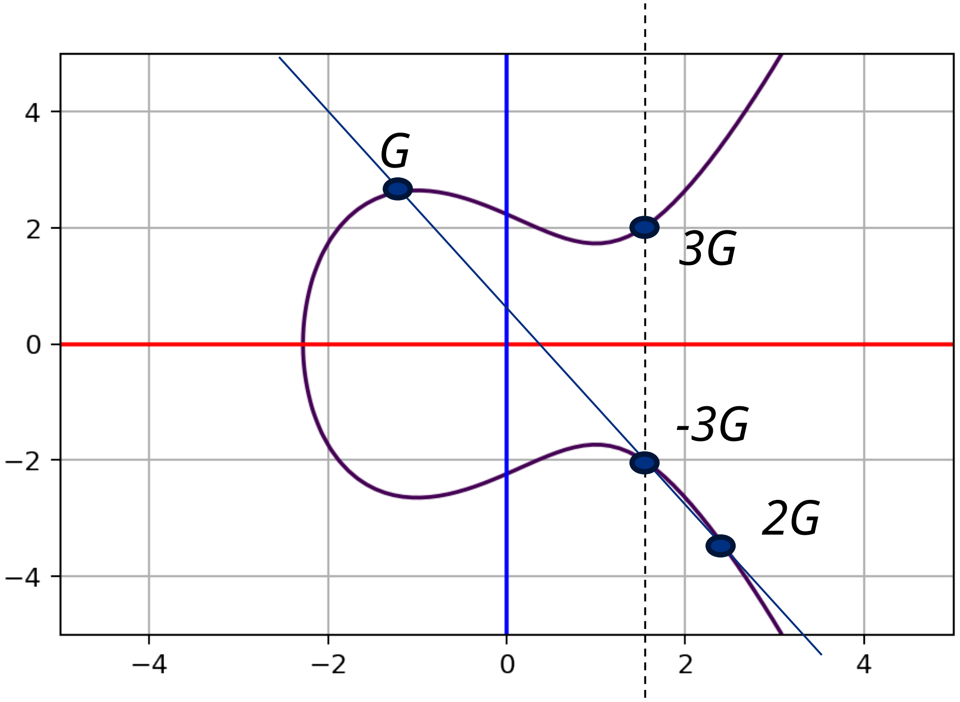
- Start with a public generator G (a point on the curve),
- walk the curve n times, publish the result



- *abGp* public key
- *n* private key

Modern ciphers – asymmetric ciphers - ECC

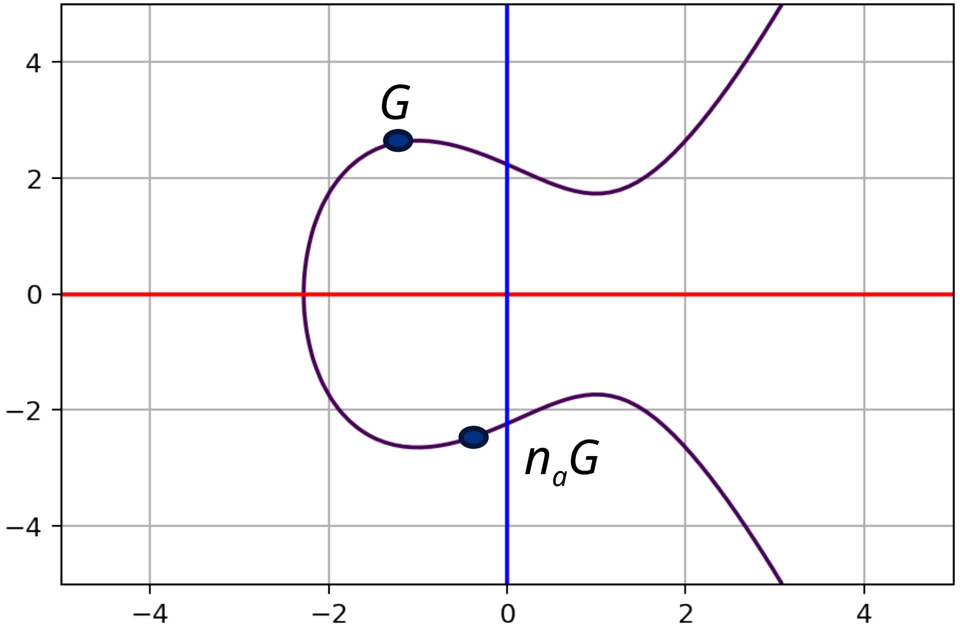




Modern ciphers – asymmetric ciphers - ECC

- How many times did you have to walk the curve to get to point *nG*? *Very* hard to calculate

- 256 bit ECC key is equivalent to 3072 bit RSA key (is equivalent to 128 bit AES)*



*read Arjen K. Lenstra's 2013 paper

Universal security

from bits and mips to pools, lakes – and beyond

Modern ciphers – asymmetric ciphers - ECC

- Alice and Bob agree on a, b, G and p

- Alice generates $n_{\mathrm{a}} \cdot G = P_{\mathrm{a}}$ and shares P_{a}

- Bob generates $n_{\mathrm{b}} \cdot G = P_{\mathrm{b}}$ and shares P_b

- Alice calculates $n_{\mathrm{a}} \cdot P_{\mathrm{b}} = n_{\mathrm{a}} \cdot (n_{\mathrm{b}} \cdot G) = K$
- Bob calculates $n_{\mathrm{b}} \cdot P_a = n_b \cdot (n_a \cdot G) = K$

- Eve calculates $P_{\mathrm{a}} \cdot P_{\mathrm{b}} = ???$

Modern ciphers – asymmetric ciphers - ECC

- NIST curves with prime fields 192, 224, 256, 384, 521 (NSA Suite B uses only 256 and 384)
  fast reduction, due to pseudo Mersenne primes like $p = 2^{521} - 1$
- NIST curves with binary fields 163, 233, 283, 409, 571
  binary fields defined by F_{2^m}
- Dual_EC_DRBG (determistic random bit generator) shenanigans

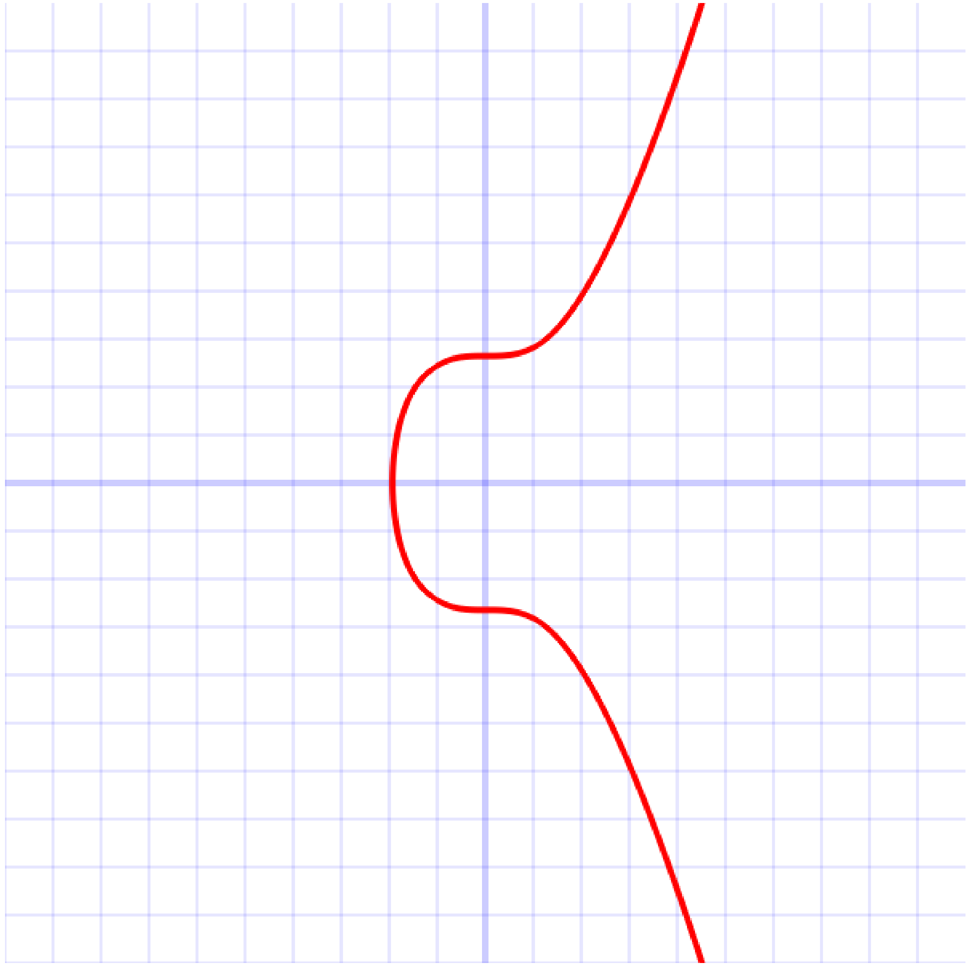
- SECG
- ECC BrainPool

- Curve25519 (Daniel J. Bernstein)
  $y^2 = x^3 + 486662x^2 + x$ (a Montgomery curve)
  over the finite field generated by $p = 2^{255} - 19$

Lame claim to fame: I had also dinner with him and Tanja Lange

Modern ciphers – asymmetric ciphers - ECC

- Bitcoin secp256k1
- $p = 2^{256} - 2^{32} - 2^{9} - 2^{8} - 2^{7} - 2^{6} - 2^{4} – 1$
- $y^2 = x^3 + 7$
- G is also defined



Future ciphers

Future ciphers

- Quantum computing
- Shor’s algorithm
- Post-quantum cryptography

Future ciphers – quantum-breaking RSA

- $N = p \cdot q$ (eg. 55)
  (remember, this is very hard for large primes)
- Pick g so GCD(N, g) = 1 (eg. 4)
- At some point, $g^r = m \cdot N + 1$

r	***g^r***	***g^r / N***	***g^r* mod *N***
1	4	0	4
2	16	0	16
3	64	1	9
4	256	4	36
5	1024	18	34
6	4096	74	26
7	16384	297	49
8	65536	1191	31
9	262144	4766	14
10	1048576	19065	1

Future ciphers – quantum-breaking RSA

- $r = 10$

- $g^r = m \cdot N + 1$ -> $g^r - 1 = m \cdot N$ -> $(g^{r/2} + 1)(g^{r/2} - 1) = m \cdot N$

  $(g^{r/2} + 1) = 4^5 + 1 = 1025$ GCD(1025, 55) = 5 (via Euclid's algorithm)

  $(g^{r/2} - 1) = 4^5 - 1 = 1023$ GCD(1023, 55) = 11

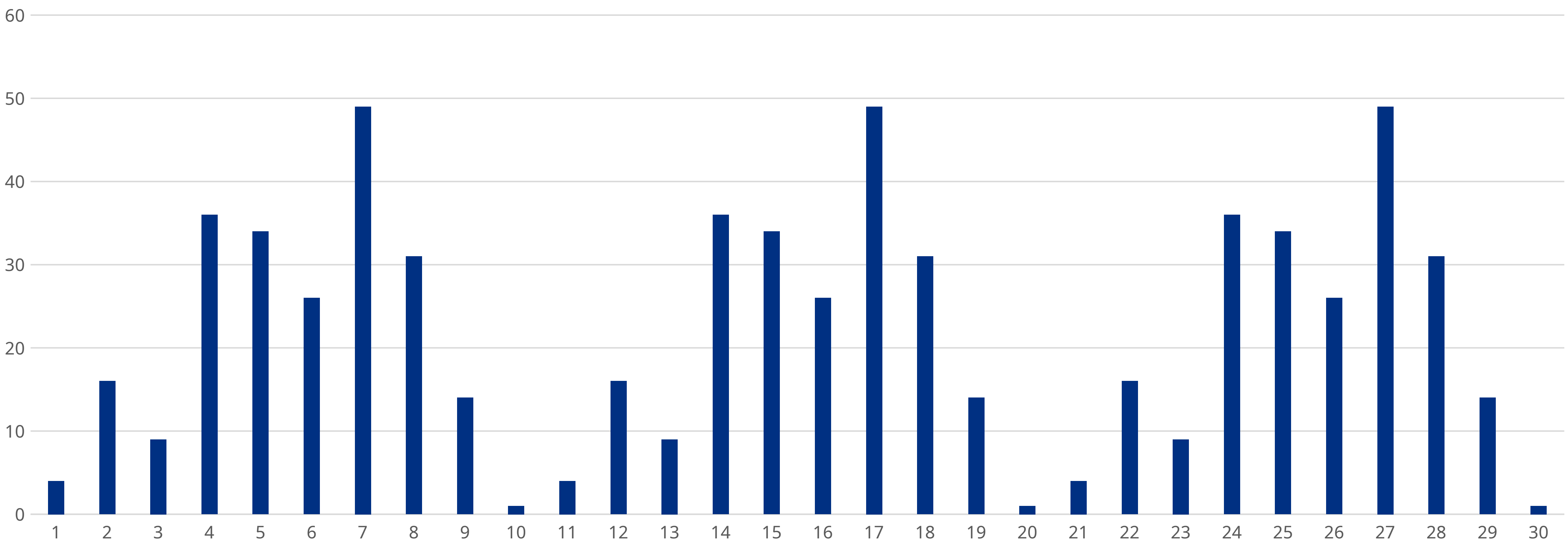
Future ciphers – quantum-breaking RSA

r	g^r	g^r / N	$g^r \bmod N$
1	4	0	4
2	16	0	16
3	64	1	9
4	256	4	36
5	1024	18	34
6	4096	74	26
7	16384	297	49
8	65536	1191	31
9	262144	4766	14
10	1048576	19065	1

r	g^r	g^r / N	$g^r \bmod N$
11	4194304	76260	4
12	16777216	305040	16
13	67108864	1220161	9
14	2.68E+08	4880644	36
15	1.07E+09	19522578	34
16	4.29E+09	78090314	26
17	1.72E+10	3.12E+08	49
18	6.87E+10	1.25E+09	31
19	2.75E+11	5E+09	14
20	1.1E+12	2E+10	1

- Periodic sequence (and $g^0 = m \cdot N + 1 = 1 \bmod N$)

Future ciphers – quantum-breaking RSA



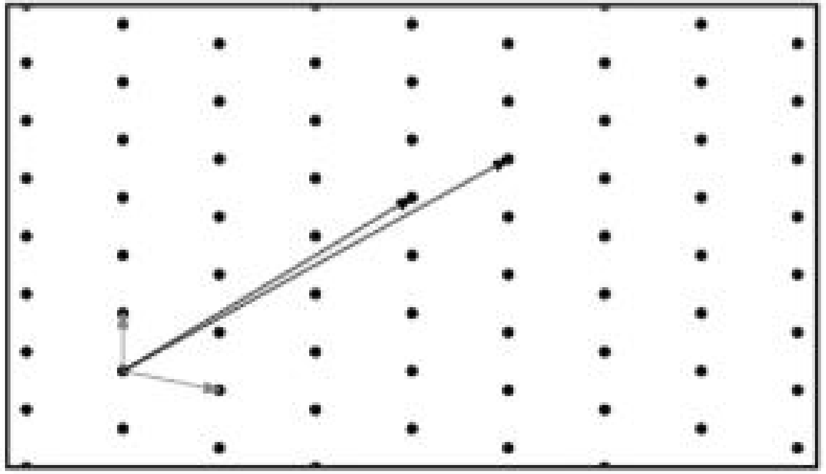
- Periodic sequence -> Use Fourier transform to find periodicity

Future ciphers – quantum-breaking RSA

- Finding periodicity (Quantum - Fast Fourier Transform)
- Factoring large numbers into prime numbers very easy (with enough qbits)
- Key exchanges no longer secret when key exchange is recorded and stored
- Cross-over point (publicly available qbits vs required qbits) somewhere in 2035…
- Symmetrical ciphers are still fine-ish

Future ciphers – Lattice-based cryptography

- Like DES and AES, NIST launched a quantum-safe algorithm competition
- 5 July 2022, 4 algorithms selected for further evaluation, 3 are lattice-based
- A lattice is a repeating grid of points in *n* dimensions
- Security is based on the shortest vector problem



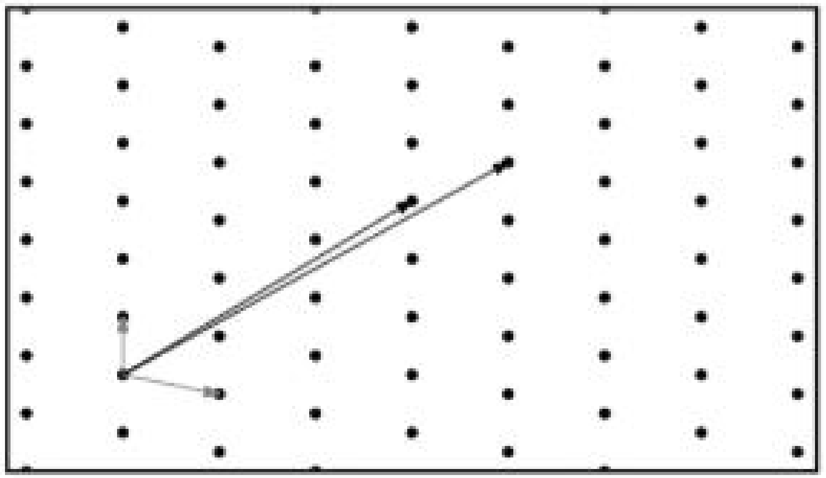
- Any resemblance with lettuce is purely coincidental

Future ciphers – Lattice-based cryptography

- Generate a lattice with simple vectors and very hard vectors

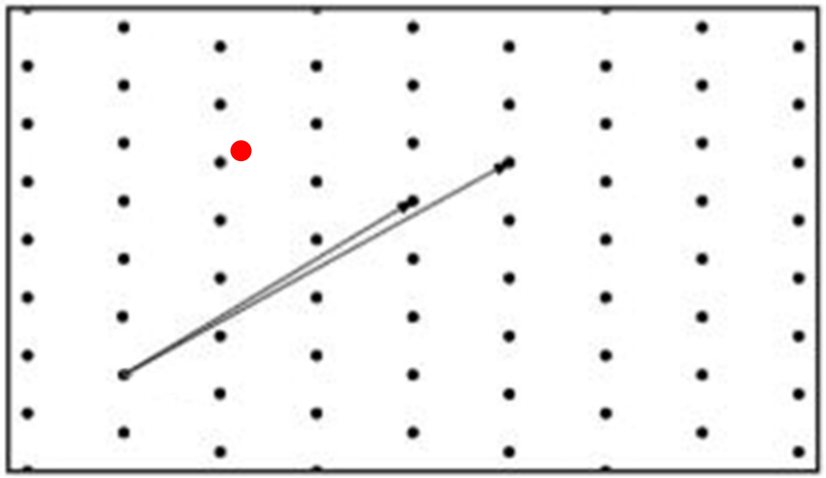
- Publish very hard vectors, keeps simple vectors secret

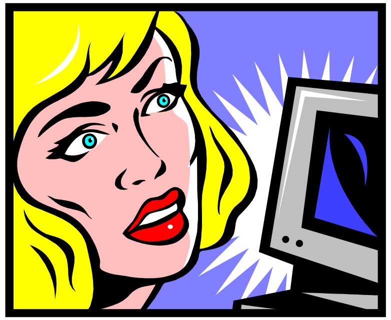
- In 1000+ dimensions



Future ciphers – Lattice-based cryptography

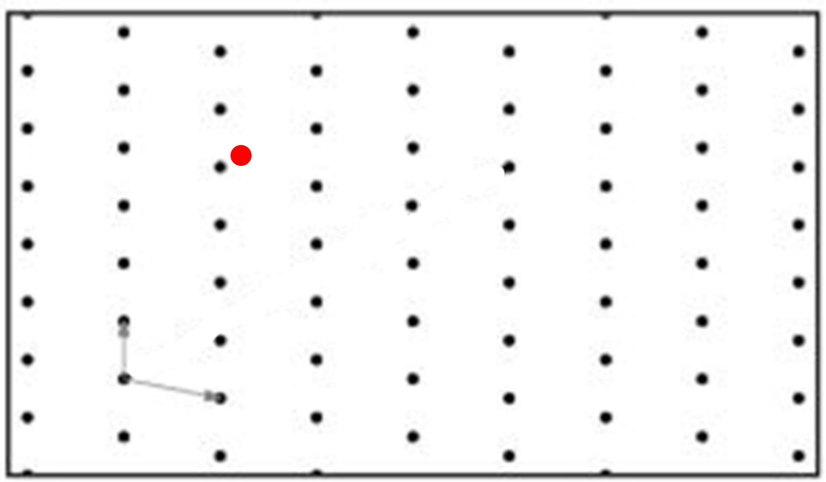
- Pick a point close to (but not on) a lattice-point that you want to share





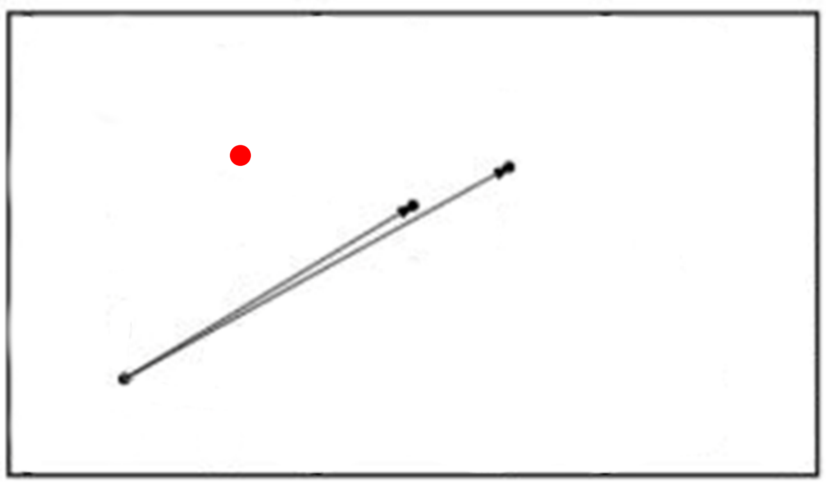
Future ciphers – Lattice-based cryptography

- Easy to find the closest lattice point with the easy vectors



Future ciphers – Lattice-based cryptography

- Very hard (also for quantum computers) to find the closest lattice point with any other vectors.



Questions?...

Questions?...

- Web
  - https://wikipedia.org
  - https://cryptii.com
  - https://www.coursera.org/learn/crypto

- Books
  - Applied Cryptography, Bruce Schneier
  - The Codebreakers, David Kahn
  - Cryptonomicon, Neal Stephenson