Cryptology - a (very) Brief Survey

Pedro Quaresma

Department of Mathematics
University of Coimbra

Belgrade 14/5/2008

Bibliography

- Stinson, Douglas, *Cryptography: Theory and Practice*, CRC, 2006.
- A. Meneses, P. van Oorschot, S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
- Buchman, Johannes, *Introduction to Cryptography*, Springer, 2000.
- Paul Garrett, *The Mathematics of Coding Theory*, Pearson, Prentice Hall, 2004.
- Richard Spillman. *Classical and Contemporary Cryptology*. Prentice Hall, 2005.

Program

- Cryptographic Quiz
- Introduction, Terminology, Kerckhoff principle
- Classic Ciphers (Cryptography & Cryptanalysis)
  - mono-alphabetic, substitution (shift,affine,permutation)
  - multi-alphabetic, substitution (Vigenère)
- Symmetric Keys systems
  - Product ciphers.
  - Fiestel blocks
  - DES, FEAL
- Cryptanalysis of Simetric Keys systems
  - Differencial
  - Linear
- Public Key systems
  - One way functions, one way functions with trapdoor
  - Goldwasser-Micali, RSA, ElGamal, Knapsack
- String Cipher
  - Vernam Cipher, one-time-pad.

Terminology

The science of cryptology is the science of secure communications, formed from the Greek words kryptós, "hidden", and lógos, "word".

Cryptography The science of the enciphering and deciphering of messages in secret code or cipher.

Cryptosystem A system for encrypting information.

Encryption The process of converting the *Plaintext* into a *Cipher*.

Decryption The process of converting the *Cipher* back into *Plaintext*.

Key The secret information known only to the transmitter and the receiver which is used to secure the *Plaintext*.

Plaintext The source information to be secured.

Ciphertext The encrypted form of the *Plaintext*.

Monoalphabetic Substitution A method of encryption where a letter in the plaintext is always replaced by the same letter in the ciphertext.

Polyalphabetic Substitution A method of encryption where a letter in the plaintext is not always replaced by the same letter in the ciphertext.

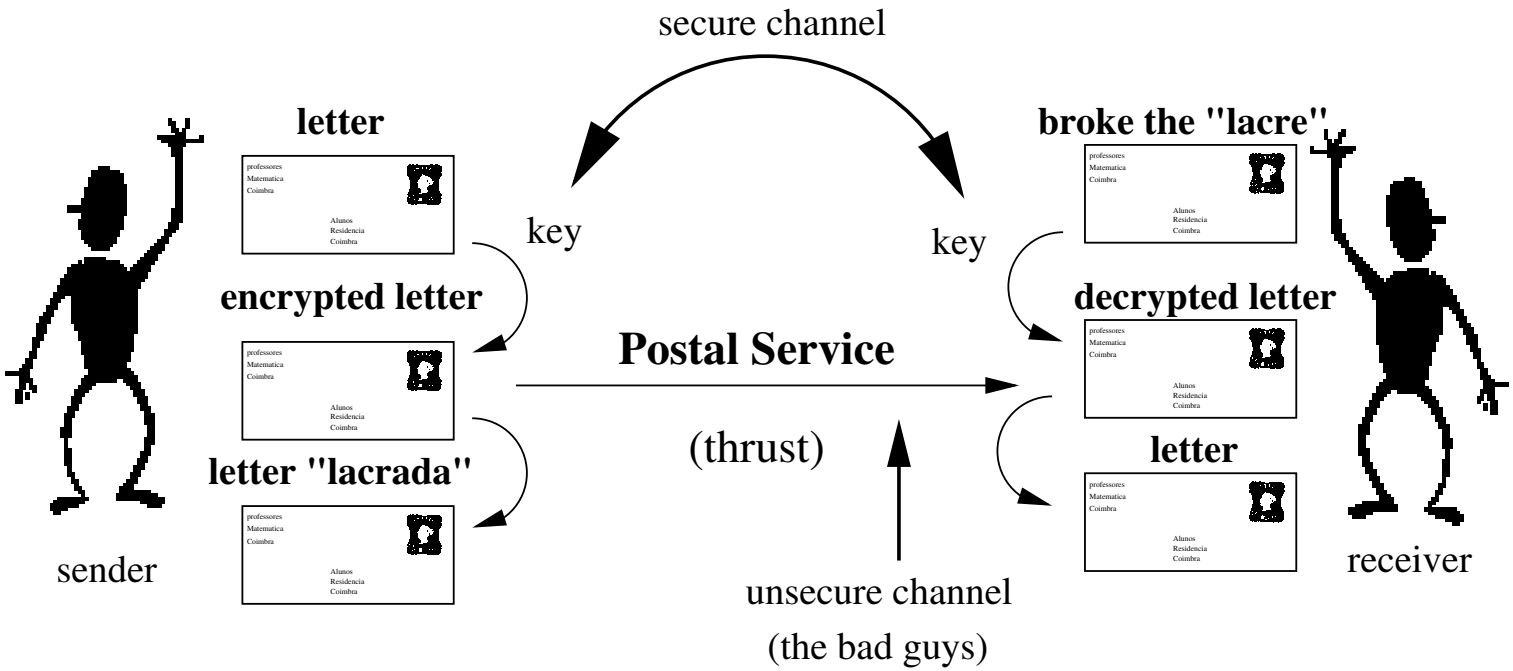
Cryptanalysis The science (and art) of recovering information from ciphers without knowledge of the key.

Code An unvarying rule for replacing a piece of information with another object, not necessarily of the same sort.

Secure Communications

- Thrust
- Protocols
- Ciphers

Lines (physical) of Communications + Computer Systems + Protocols + Law



Kerckhoffs (1835-1903) Laws

1. The system must be practically, if not mathematically, indecipherable;
2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;
3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;
4. It must be applicable to telegraphic correspondence;
5. It must be portable, and its usage and function must not require the concourse of several people;
6. Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

The second principle is best known as *Kerckhoffs' principle*.

Kerckhoffs' principle

Definition (Kerckhoffs' principle)

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

Block Ciphers & Symmetric Keys

Definition (Block Cipher)

A block cipher *is a cipher where the plain text is split in blocks of a given fixed size t. The encryption is made block by block, repeating the same procedure every time.*

Definition (Symmetric Keys Ciphers)

Given a cipher system, defined by an encryption, and an decryption functions, $\{E_e : e \in \mathcal{K}\}$ and $\{D_d : d \in \mathcal{K}\}$, where $\mathcal{K}$ is the Key space*. We say that the cipher is* symmetric keys cipher *if for any pair of keys (e, d), it is computacionaly "easy" to get d knowing (only) the values of e, and also get e from d.*

Shift Cipher

Julius Caesar (100bc-44bc), shift letters position by three.

$$e = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m \\ d & e & f & g & h & i & j & k & l & m & n & o & p \\ \\ n & o & p & q & r & s & t & u & v & w & x & y & z \\ q & r & s & t & u & v & w & x & y & z & a & b & c \end{pmatrix}$$

Definition (Shift Cipher)

Given $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. *For* $0 \leq K \leq 25$, *we have:*

$$e_K(x) = (x + K) \mod 26$$

e

$$d_K(y) = (y - K) \mod 26$$

for all $x, y \in \mathbb{Z}_{26}$

Affine Cipher

Definition (Affine Cipher)

Given $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}$, *and:*

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} \ : \ \gcd(a, 26) = 1\}.$$

For $K = (a, b) \in \mathcal{K}$, *we define:*

$$e_k(x) = (ax + b) \mod 26$$

and

$$d_k(y) = a^{-1}(y - b) \mod 26$$

for all $x, y \in \mathbb{Z}_{26}$

Polyalphabetic Cipher

Definition (Polyalphabetic Substitution Cipher)

A Polyalphabetic Substitution Cipher, *with a block length, t, for a given alphabet $\mathcal{A}$ its a cipher such that:*

1. *the key space $\mathcal{K}$ is formed by all the ordered sets of t permutations $(p_1, p_2, \ldots, p_t)$, where each of the permutations p_i is defined in the set $\mathcal{A}$;*
2. *the encryption of the message $m = (m_1 m_2 \ldots m_t)$ with key $e = (p_1, p_2, \ldots, p_t)$ is given by $E_e(m) = (p_1(m_1)p_2(m_2)\ldots p_t(m_t))$;*
3. *the decryption key corresponding to $e = (p_1, p_2, \ldots, p_t)$ is $d = (p_1^{-1}, p_2^{-1}, \ldots, p_t^{-1})$.*

Vigenère Cipher

Vigenère Cipher

Given $\mathcal{A} = \{a, b, c, \ldots, x, z\}$ and $t = 3$. Let $e = (p_1, p_2, p_3)$ be such that p_1 maps the letters of $\mathcal{A}$ in letters three positions to the right, p_2 seven positions, and p_3 ten positions. Then

$$m = \text{est aci fra nao ese gur axx}$$

is transformed in

$$c = E_e(m) = \text{hbf djt ial qha hbp jdd dfi}$$

Notice the ambiguous filling on the last block. How can we define a unambiguous filling?

Cryptanalysis - Goals

Cipher (partially) broken The main goal of the adversary is to recover, in a systematic form, the plain text given a encrypted text. If this goal is attained we say that the cipher was (partially) broken.

Cipher Broken A more ambitious goal is to get the secret key(s). It that happens, then the cipher was broken.

Brute Force Attack

For symmetric-key ciphers, a brute force attack typically means a brute-force search of the key space; that is, testing all possible keys in order to recover the plaintext used to produce a particular ciphertext.

If a cipher is breakable by such an attack, then it is an (extremely) weak cipher.

All the classical cipher are weak ciphers.

- Shift Cipher - $|\mathcal{A}|$
- Affine Cipher - $\varphi(|\mathcal{A}|) * |\mathcal{A}| + |\mathcal{A}|$
- Vigenère Cipher - $|\mathcal{A}|^{|\mathcal{A}|}$

Frequency Analysis

In a simple substitution cipher, each letter of the plaintext is replaced with another, and any particular letter in the plaintext will always be transformed into the same letter in the ciphertext. For instance, if all occurrences of the letter e turn into the letter x, a ciphertext message containing numerous instances of the letter x would suggest to a cryptanalyst that x represents e (in English).

- Letter frequencies
- Digrams, Trigrams
- Initial and final letters of words
- small words: one, two, three letters words.
- Index of Coincidence; Mutual Index of Coincidence.

Frequency Analysis

An example with a mono-alphabetic substitution cipher.

Pedro Quaresma and Augusto Pinho, *Análise de Frequências da Língua Portuguesa*, InterTIC 2007, 3-5 Dec, Porto, Portugal.

Breaking Vigenère Cipher

ADÃO E EVA NO PARAÍSO

Adão, Pai dos Homens, foi criado no dia 28 de Outubro. às duas horas da tarde... Assim o afirma, com majestade, nos seus ≪Annales Veteris et Novi Testamenti≫, o muito douto e muito ilustre Usserius, bispo de Meath, arcebispo de Armagh, e chanceler-mor da Sé de S. Patrício.

shdí e iôv né évzakwè

shdí, êez loò yí ueèw, noà tôqavs ì w vmr 28 hv wuóysôw. çí lusw âwrsw yi óeì ym... vàsàq í axmìêi, gèê msnvõáavi, voò í zâs ≪vvnspvõ vwxvôqs io voõm ùmsóeãzvtà≫, w çyzùw vsóùw w ãúqté zéâsóvv âsòiiãâs, sãàpé uz mweòâ, svtzjiòtè le eìêigz, z czeçxmlwv-êwr hr àé hv à. trùzíumè.

1. First task - to get the key length $\longrightarrow$ Index of Coincidence.

Index of Coincidence

Definition (Index of Coincidence)

Given $x = x_1 x_2 \ldots x_n$ a string of n alphabetic characters. The index of coincidence *of x, denoted $IC(x)$, is defined to be the probability that two random elements of x are identical.*

$$IC(x) = \frac{\sum_{i=1}^{|\mathcal{A}|} \binom{f_i}{2}}{\binom{n}{2}} = \frac{\sum_{i=1}^{|\mathcal{A}|} f_i(f_i - 1)}{n(n-1)}$$

$$IC(Pt) \approx \sum_{i=0}^{|\mathcal{A}|} p_i^2 = 0.069609$$

$$IC(\text{random string}) \approx |\mathcal{A}| \left(\frac{1}{|\mathcal{A}|}\right)^2 = \frac{1}{|\mathcal{A}|} = 0.038$$

Breaking Vigenère Cipher - II

```
length 1, IC value = 0.035673
length 2, IC value = 0.042503
length 3, IC value = 0.054156
length 4, IC value = 0.042462
length 5, IC value = 0.035637
length 6, IC value = 0.076101

The key length should be 6

CPU: 0.02s
```

$$K = (k_1, k_2, k_3, k_4, k_5, k_6)$$

2. Second task - to break the key $\longrightarrow$ Mutual Index of Coincidence.

Mutual Index of Coincidence

Definition (Mutual Index of Coincidence)

The mutual index of coincidence *of x and y, denoted $mIC(x, y)$, is defined as the probability that a random element of x is identical to a random element of y.*

If we choose, as reference, the probabilities of the language in question, we have:

$$mIC(Pt, y_i)_j = \sum_{i=1}^{|\mathcal{A}|} \frac{p_i f_{i+j}}{n'}, \qquad 1 \leq j \leq |\mathcal{A}|, n' = \text{length}(y_i)$$

if $j = k_i$, then we would expect that

$$mIC(Pt, y_i)_{k_i} \approx \sum_{i=1}^{|\mathcal{A}|} p_i^2 = 0.069609$$

For values $j \neq k_i$ the value found will be significantly smaller.

Breaking Vigenère Cipher - III

```
Text 1 - YvÒÓÙÀÌÒÍÚÀÀÇÌÀÒzzÓÙwÓçÀzÀÒÜÒÕywÕÙwzÍÙy7 ...
Text 2 - woúùÙèóxó0ôóòòáÙèúQááùòÙùàù0ÀìùÙÙTçíxóáü ...
Text 3 - éOÉCú6E0C6ó7óADD7D820fùCóóhùC819úCCü8ôóC ...
Text 4 - ÓOFFùü79üüùô86Fô9Cü1üúEôÉ99ü7üúü8üôôE30ô ...
Text 5 - ÔÚ716D19BDbôòBù5DAùùõùd6üùD7CBEAùÉÂôDùA1 ...
Text 6 - wôóüÙTò0ÜíÜóùÜòáùÙóúÚúáçóìÊúáôÙÙùÙáÙòòùô ...
```

```
R1 - ...; mIC_17=0.0245; mIC_18=0.0548; mIC_19=0.0388; ...
R2 - ...; mIC_3=0.0356; mIC_4=0.0765; mIC_5=0.0368; ...
R3 - ...; mIC_16=0.0215; mIC_17=0.0500; mIC_18=0.0308; ...
R4 - ...; mIC_20=0.0277; mIC_21=0.0529; mIC_22: 0.0351; ...
R5 - ...; mIC_7=0.0328; mIC_8=0.0642; mIC_9=0.0261; ...
R6 - mIC_0=0.0750; mIC_1=0.0371; mIC_2=0.0290; ...
```

The key: (18,4,17,21,8,0), “servia”.

Transposition Ciphers

Another type of ciphers are the *transposition ciphers*, in which the symbols in each block are permuted.

Definition (Transposition Ciphers)

Given a block cipher with a block of length t. Given $\mathcal{K}$ the set of all permutations in the set $\{1, 2, \ldots, t\}$. For each $e \in \mathcal{K}$ we can define the encryption function:

$$E_e(m) = (m_{e(1)} m_{e(2)} \ldots m_{e(t)})$$

where $m = (m_1 m_2 \ldots m_t) \in \mathcal{M}$.
The resulting cipher is a transposition cipher, *with key e. The deciphering is made with the inverse permutation $d = e^{-1}$.*

A transposition, by itself, preserve the symbols in each block, and as a consequence of this, is easy to break.

Product Cipher

The substitution and transposition cipher are weak cipher, their combination give rises to a stronger cipher.

Product Cipher

Let $\mathcal{M} = \mathcal{C} = \mathcal{K}$ be the set of all bit streams off length 6. $|\mathrm{M}\| = 2^6 = 64$. Let $m = (m_1 m_2 \ldots m_6)$, and:

$$\begin{aligned} E_k^{(1)}(m) &= m \oplus k, \text{aonde } k \in \mathcal{K}, \\ E^{(2)}(m) &= (m_4 m_5 m_6 m_1 m_2 m_3). \end{aligned}$$

$E_k^{(1)}$ it is a substitution polyalphabetic cipher, $E^{(2)}$ it is a transposition cipher. The product of the two ciphers is given by: $E_k^{(1)} E^{(2)}$.

This type of product cipher is call "a round".

Confusion and Diffusion

Definition (Confusion)

A cipher is said, to add confusion *when the complexity between the key and the encrypted text raises. A substitution cipher adds confusion to a product cipher.*

Definition (Diffusion)

A cipher is said to add diffusion *when there is a spreading of the "bits" in the message in such a way that any redundancy in the text is spread along the text itself. A transposition cipher adds diffusion to a product cipher.*

A round adds confusion and diffusion to a cipher.

Substitution-Permutation Network

Definition (Substitution-Permutation Network)

A substitution-permutation network *it is a product cipher built up from several levels of substitutions and permutations.*

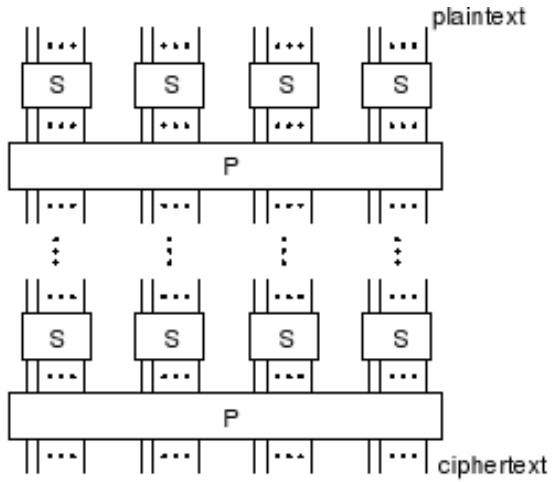


Figure 7.7: *Substitution-permutation (SP) network.*

Iterated Block Cipher

Definition (Iterated Block Cipher)

A iterated block cipher *it is a block cipher with an iterated application of an internal function, designated "round function".*
The parameters of this cipher are: the number of rounds r, the length in bits of the block n, the length in bits of the key k, of the input key K, from which r sub-keys K_i (rounds keys) are built.
For each of the sub-keys the round function should be a bijection.

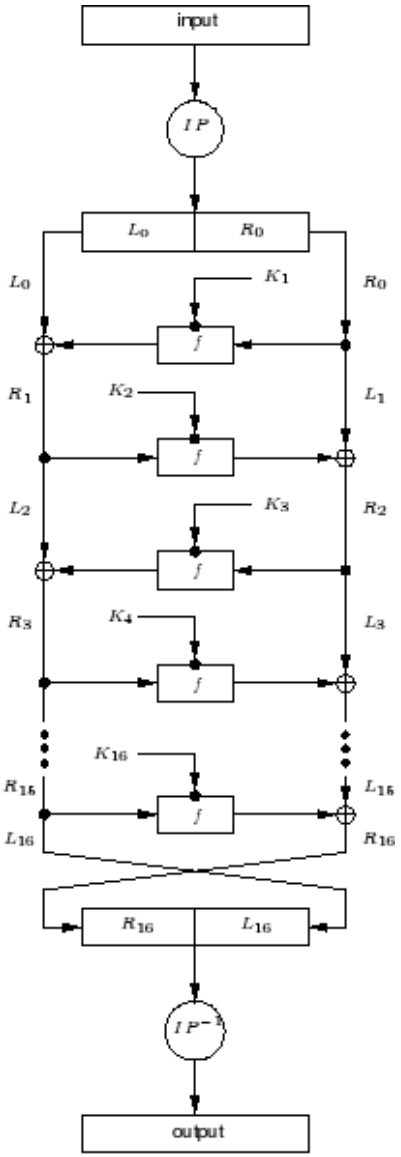
Feistel Cipher

Definition (Feistel Cipher)

A Fiestel cipher *it is an iterated block cipher that has as input a plain text of* $2t$*-bits* (L_0, R_0)*, where* L_0 *e* R_0 *are blocks with* t *bits, in a encrypted text* (R_r, L_r)*, through a process with* r *rounds, where* $r \geq 1$*.*

For $1 \leq i \leq r$*, the round* i *applies* $(L_{i-1}, R_{i-1}) \xrightarrow{K_i} (L_i, R_i)$ *in:* $L_i = R_{i-1}$*,* $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$*, where each one of the sub-keys* K_i *is derived from the cipher's key* K*.*

Feistel Cipher



$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

Feistel Cipher

Usually $r \geq 3$, with r, even.

Note that the last step switch the blocks, the output is (R_r, L_r) and not (L_r, R_r);

The decryption is made reverting the process with the order of the keys also reversed.

The f function of the Feistel cipher could be a product cipher, it does not need to be invertible to the all Fiestel cipher be invertible.

Feistel Ciphers

DES "**D**ata **E**ncryption **S**tandard", is a cipher selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally.

FEAL "**F**ast Data **E**ncipherment **Al**gorithm", is a block cipher proposed as an alternative to the Data Encryption Standard (DES), and designed to be much faster in software. The Feistel based algorithm was first published in 1987 by Akihiro Shimizu and Shoji Miyaguchi from NTT.

IDEIA "**I**nternational **D**ata **E**ncription **Al**gorithm", is a block cipher designed by Xuejia Lai and James Massey of ETH Zurich and was first described in 1991. The algorithm was intended as a replacement for the Data Encryption Standard.

This ciphers are susceptible to various forms of cryptanalysis, namely, differential and linear cryptanalysis.

FEAL

Fast Data **E**ncipherment **Al**gorithm, is a block cipher proposed as an alternative to the Data Encryption Standard (DES), and designed to be much faster in software. The Feistel based algorithm was first published in 1987 by Akihiro Shimizu and Shoji Miyaguchi from NTT.

The cipher is susceptible to various forms of cryptanalysis, and has acted as a catalyst in the discovery of differential and linear cryptanalysis.

- FEAL-4, the first version.
- FEAL-N, a 64bits key and N rounds. The $N = 2^x$ can be chosen by the user;
- FEAL-NX, a 128bits key, and N rounds.

Algorithm FEAL

Algorithm FEAL-8

INPUT: plain text: 64 bits, $M = m_1 \dots m_{64}$; key: 64 bits $K = k_1 \dots k_{64}$

OUTPUT: Cipher text: 64 bits, $C = c_1 \dots c_{64}$.

1. Build sixteen sub-keys of 16 bits K_i from the K.
2. Define $M_L = m_1 \dots m_{32}$, $M_R = m_{33} \dots m_{64}$.
3. $(L_0, R_0) \leftarrow (M_L, M_R) \oplus ((K_8, K_9), (K_{10}, K_{11}))$. (XOR of the initial sub-keys)
4. $R_0 \leftarrow R_0 \oplus L_0$.

Algorithm FEAL (part II)

Algorithm FEAL-8 (part II)

5. For i from 1 to 8 do: $L_i \leftarrow R_{i-1}$, $R_i \leftarrow L_{i-1} \oplus f(R_{i-1}, K_{i-1})$. (Using the given table to get $f(A, Y)$ with $A = R_{i-1} = (A_0, A_1, A_2, A_3)$ e $Y = K_{i-1} = (Y_0, Y_1)$.)
6. $L_8 \leftarrow L_8 \oplus R_8$.
7. $(R_8, L_8) \leftarrow (R_8, L_8) \oplus ((K_{12}, K_{13}), (K_{14}, K_{15}))$. (XOR of the final sub-keys)
8. $C \leftarrow (R_8, L_8)$. (The order of the last blocks is switched)

FEAL — Building the Sub-Keys

FEAL-8 — Building the Sub-Keys

INPUT: 64 bits key, $K = k_1 \ldots k_{64}$.
OUTPUT: Extended Key, 256 bits, 16 sub-keys, each with 16 bits K_i, $0 \leq i \leq 15$).

1. $U^{(-2)} \leftarrow 0$, $U^{(-1)} \leftarrow k_1 \ldots k_{32}$, $U^{(0)} \leftarrow k_{33} \ldots k_{64}$ (initialisation).
2. $U \stackrel{\text{def}}{=} (U_0, U_1, U_2, U_3)$ for U_i with 8 bits. Calculate $K_0, \ldots, K_{15}$ with i from 1 to 8:
   1. $U \leftarrow f_K(U^{(i-2)}, U^{(i-1)} \oplus U^{(i-3)})$. (with f_K defined by a table, where A e B denote 4 bits' vectors (A_0, A_1, A_2, A_3), (B_0, B_1, B_2, B_3))
   2. $K_{2i-2} = (U_0, U_1)$, $K_{2i-1} = (U_2, U_3)$, $U^{(i)} \leftarrow U$.

FEAL — Example

FEAL — Example

For a given plain text (in hexadecimal)
$M = 00000000\ 00000000$ and key $K = 01234567\ 89ABCDEF$,
the sub-keys algorithm gives the sub-keys $(K_0, \ldots, K_7) = DF3BCA36\ F17C1AEC\ 45A5B9C7\ 26EBAD25$,
$(K_8, \ldots, K_{15}) = 8B2AECB7\ AC509D4C\ 22CD479B\ A8D50CB5$.

The algorithm FEAL-8 creates the ciphertext
$C = CEEF2C86\ F2490752$.

For the FEAL-16, we will have $C = 3ADE0D2A\ D84D0B6F$.

For the FEAL-32 $C = 69B0FAE6\ DDED6B0B$.

Cryptoanalysis of Fiestel Ciphers

M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology - EUROCRYPT'93 (LNCS no. 765), Springer-Verlag, pp. 386-397, 1994.

E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, vol. 4, no. 1, pp. 3-72, 1991.

Howard M. Heys, *A Tutorial on Linear and Differential Cryptanalysis*, Memorial University of Newfoundland, Canada, (Internet)

Linear Cryptanalysis

Linear cryptanalysis tries to take advantage of high probability occurrences of linear expressions involving plaintext bits, "ciphertext" bits, and subkey bits.

- It is a **known plaintext attack**:
  - the attacker has the information on a set of plaintexts and the corresponding ciphertexts.
  - the attacker has no way to select which plaintexts (and corresponding ciphertexts) are available.

Linear Cryptanalysis

The basic idea is to approximate the operation of a portion of the cipher with an expression that is linear where the linearity refers to a mod-2 bit-wise operation. Such an expression is of the form:

$$X_{i_1} \oplus X_{i_2} \oplus \cdots \oplus X_{i_u} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \cdots \oplus Y_{j_v} = 0$$

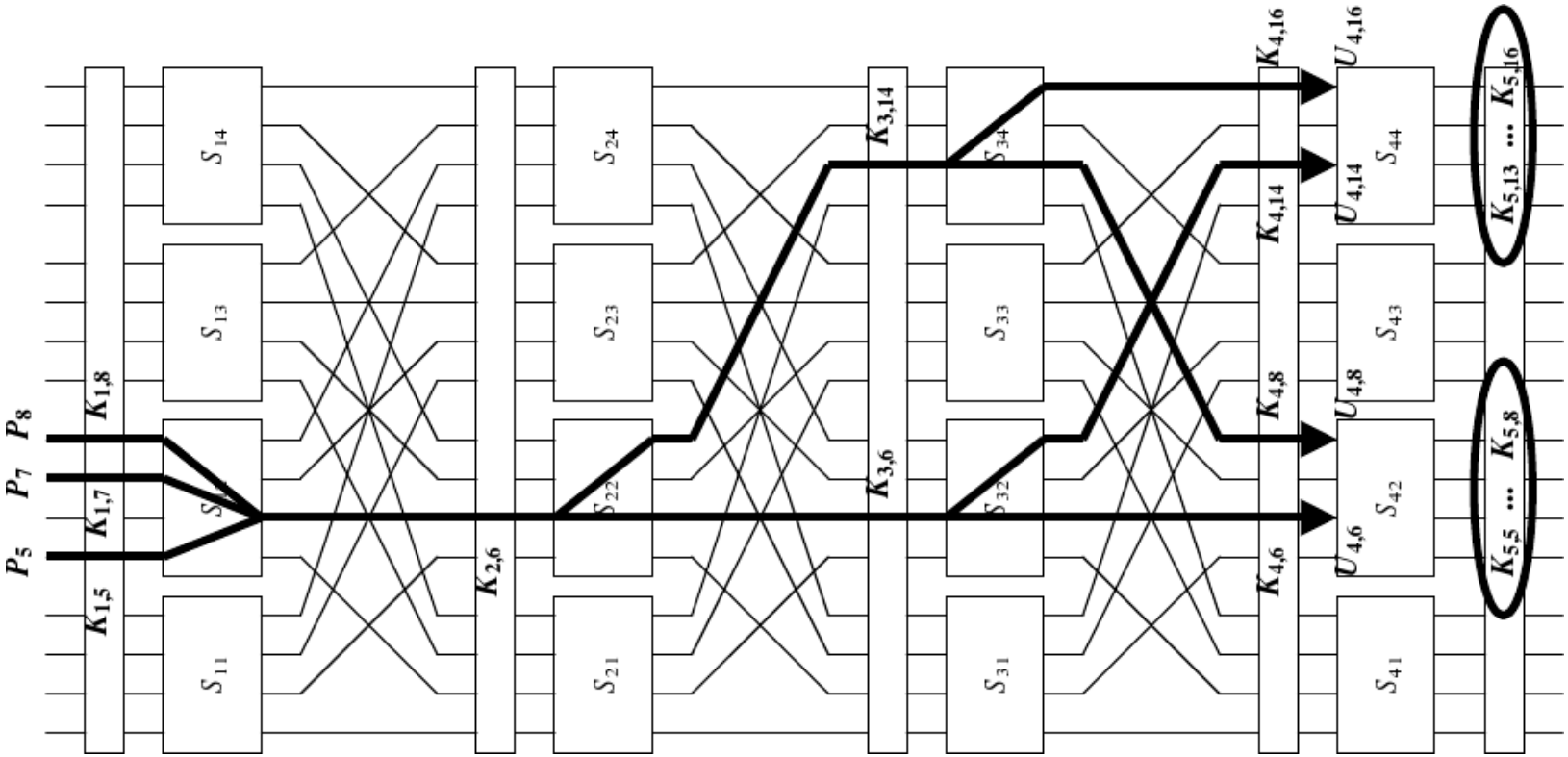
where X_i represents the i-th bit of the input $X = [X_1, X_2, \ldots]$ and Y_j represents the j-th bit of the output $Y = [Y_1, Y_2, \ldots]$.

The approach in linear cryptanalysis is to determine expressions of the form above which have a high or low probability of occurrence.

Consider that if we randomly selected values for u + v bits and placed them into the equation above, the probability that the expression would hold would be exactly $1/2$.

It is the deviation or bias from the probability of $1/2$ for an expression to hold that is exploited in linear cryptanalysis.

Linear Crytanalysis



Linear Cryptanalysis vs. FEAL

cipher	data complexity know plaintexts	storage complexity	processing complexity
FEAL-4	5	30KB	6min
FEAL-6	100	100KB	40min
FEAL-8	2^{24}	280KB	10min

Differencial Crytanalysis

Differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher.

- It is a **chosen plaintext attack**
  - the attacker is able to select inputs and examine outputs in an attempt to derive the key.
  - the attacker will select pairs of inputs, $X'$and X'', to satisfy a particular ΔX, knowing that for that ΔX value, a particular ΔY value occurs with high probability.

Differencial Crytanalysis

For example, consider a system with input $X = [X_1 X_2 \dots X_n]$ and output $Y = [Y_1 Y_2 \dots Y_n]$. Let two inputs to the system be X' and X'' with the corresponding outputs Y' and Y'', respectively. The input difference is given by $\Delta X = X' \oplus X''$, hence

$$\Delta X = [\Delta X_1 \Delta X_2 \dots \Delta X_n]$$

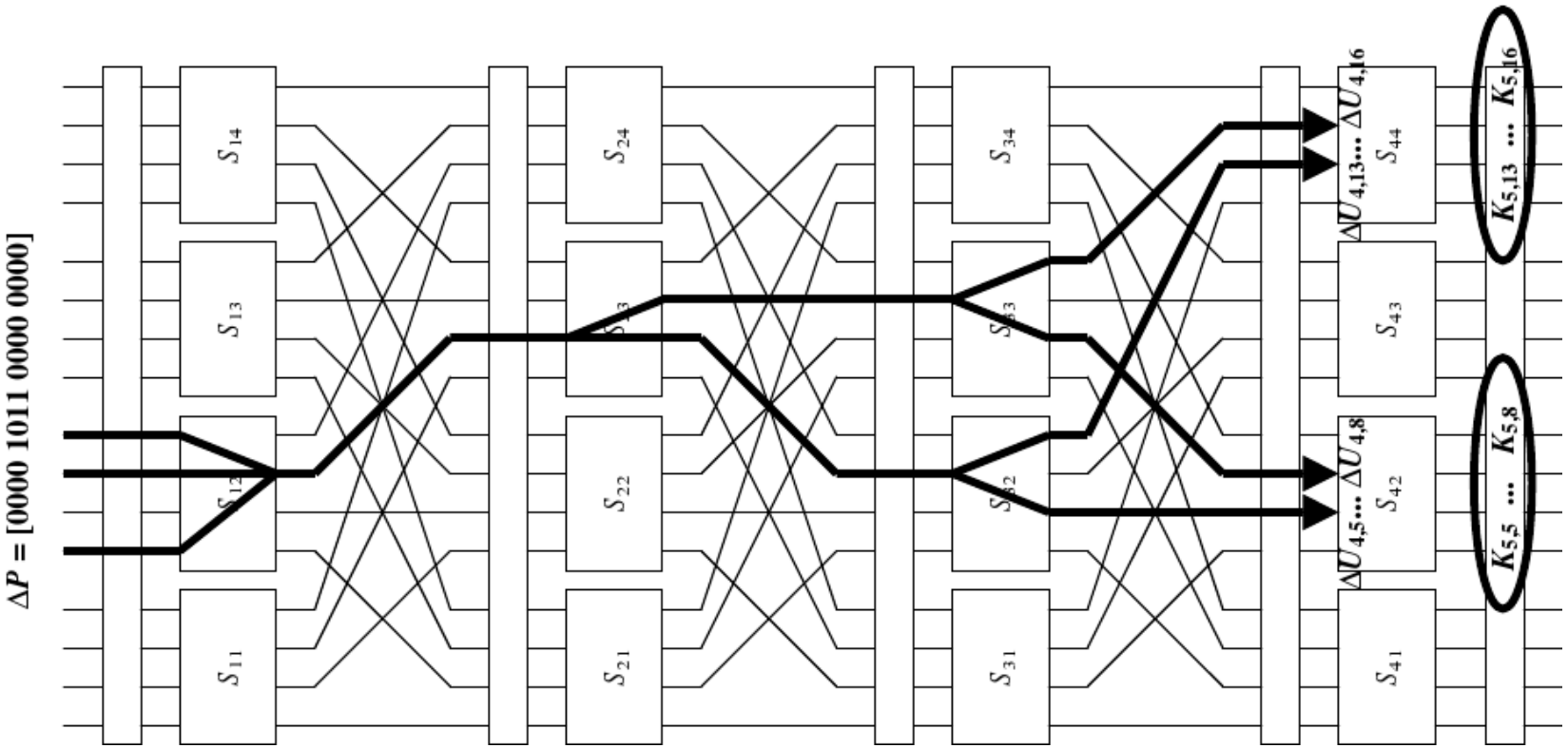
where $\Delta X_i = X'_i \oplus X''_i$.
Similarly, $\Delta Y = Y' \oplus Y''$ is the output difference and

$$\Delta Y = [\Delta Y_1 \Delta Y_2 \dots \Delta Y_n]$$

where $\Delta Y_i = Y'_i \oplus Y''_i$.
In an ideally randomizing cipher, the probability that a particular output difference ΔY occurs given a particular input difference ΔX is $1/2^n$ where n is the number of bits of X.

Differential cryptanalysis seeks to exploit a scenario where a particular ΔY occurs given a particular input difference ΔX with a very high probability p_D (i.e., much greater than $1/2^n$). The pair $(\Delta X, \Delta Y)$ is referred to as a differential.

Differencial Crytanalysis



FEAL Strength Against DC

cipher	data complexity chosen plaintexts	storage complexity	processing complexity
FEAL-8	2^7 pairs	—	2min
FEAL-16	2^{29} pairs	—	2^{30} operations
FEAL-24	2^{45} pairs	—	2^{46} operations
FEAL-32	2^{66} pairs	—	2^{67} operations

Pros & Cons of Symmetric Keys Ciphers

Pros

1. high throughput.
2. small keys.
3. can be used as primitives in larger systems.
4. easy to be combined to build a stronger system.
5. already with a large history.

Cons

1. The keys of all entities involved has to be kept secret.
2. If the number of entities is large, so it is the number of keys.
3. The keys should be changed very frequently.

One-Way Function

Definition (One-Way Function)

A $X \xrightarrow{f} Y$ *is said to be a one-way function if* $f(x)$ *is "easy to compute" for all the* $x \in X$*, but "essentially for all"* $y \in \mathrm{Im}(f)$ *it is "hard to compute" finding the* $x \in X$ *such that* $f(x) = y$*.*

- "easy to compute" and "hard to compute" can be defined in a formal way.
- "essentially for all" means that, some elements $y \in Y$ may exist for which it will be easy to compute the $x \in X$ such that $y = f(x)$.

One-Way Function — Example

One-Way Function

Let $p = 48611$ and $q = 53993$ be two prime numbers, $n = pq$, and $X = \{1, 2, \ldots, n-1\}$. Given $f(x) = r_x$, $x \in X$ where r_x it is the remainder of the division of 3^x by n.

Compute $f(x)$ is easy.

If the prime factors of n are unknown and large, the inverse problem is very hard to compute.

If the prime factors of primes n, p e q are known, to compute $y = f(x)$ can be done in a efficient way.

Trapdoor One-Way Function

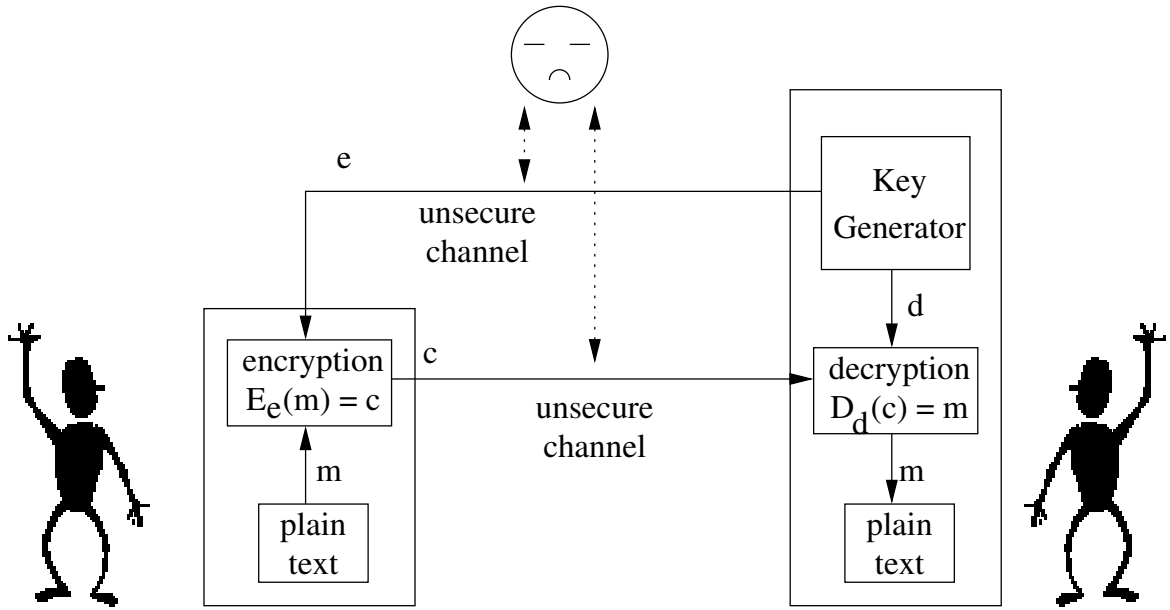
Definition (Trapdoor One-Way Function)

A trapdoor one-way function *it is a one-way function* $f : X \longrightarrow Y$ *with the property that, with some additional information, it becames easy to find, for a given* $y \in \mathrm{Im}(f)$, *an* $x \in X$ *such that* $f(x) = y$.

Public Key Ciphers are Trapdoor One-Way Functions.

Public Keys Ciphers

In a public keys Cipher we need to know the receiver public key to send the message. Only the receiver with the secret key is able to decipher the message.
The key can be sent over an unsecure channel.



Public Keys Ciphers

Goldwasser-Micali - The GM cryptosystem is semantically secure based on the assumed intractability of the **quadratic residues** problem modulo a composite $N = pq$ where p, q are large primes. The quadratic residue problem is easily solved given the factorisation of N.

RSA - The security of the RSA cryptosystem is based on the problem of **factoring large numbers**. Full decryption of an RSA ciphertext is thought to be infeasible on the assumption that this problem is hard, i.e., no efficient algorithm exists for solving them.

ElGamal - ElGamal encryption can be defined over any cyclic group G. Its security depends upon the difficulty of a certain problem in G related to computing **discrete logarithms**.

Knapsack - the **subset sum problem**, given a set of integers and an integer s, does any non-empty subset sum to s?

Goldwasser-Micali Cipher

Goldwasser-Micali - The Goldwasser-Micali cryptosystem (GM) is an asymmetric key encryption algorithm developed by Shafi Goldwasser and Silvio Micali in 1982.

GM has the distinction of being the first *probabilistic public-key encryption scheme* which is provably secure under standard cryptographic assumptions.

However, it is not an efficient cryptosystem, as ciphertexts may be several hundred times larger than the initial plaintext.

The GM cryptosystem is semantically secure based on the assumed intractability of the quadratic residues problem modulo a composite $N = pq$ where p, q are large primes.

G-M Cipher — Key Generation

Key Generation

Each entity A has to do the following:

1. Choose two distinct primes p e q, with similar length.
2. Compute $n = pq$.
3. Choose a $y \in \mathbb{Z}_n$ such that y it is a non-quadratic residue modulus n and $\left(\frac{y}{n}\right) = 1$ (y it is pseudo-quadratic residue of n)
4. The public key of A is (n, y); the private key of A is (p, q).

G-M Cipher — Encryption

The sender B encrypt the message m to the receiver A.

G-M Cipher — Encryption

Encryption: B should do the following:

1. Gets the public key of A, (n, y).
2. Represents the message m as a binary sequence $m = m_1 m_2 \ldots m_t$ of length t.
3. **For** $i \leftarrow 1$ **to** t **do**
   1. choose randomly an $x \in \{1, \ldots, n-1\}$ prime with n.
   2. **If** $m_i = 1$ **then** $c_i \leftarrow yx^2 \mod n$ **else** $c_i \leftarrow x^2 \mod n$.
4. sends the t-tuplo $c = (c_1, c_2, \ldots, c_t)$ to A.

G-M Cipher — Decryption

Goldwasser-Micali Cipher — Decryption

Decryption: A should do the following:

1. **For** $i \leftarrow 1$ **to** t **do**
   1. $e_i \leftarrow \left(\frac{c_i}{p}\right)$
   2. **If** $e_i = 1$ **then** $m_i \leftarrow 0$ **else** $m_i \leftarrow 1$.
2. The decrypted message is $m = m_1 m_2 \ldots m_t$.

G-M Cipher — Proof of Correctness

Proof of correctness, $E^{-1}(E(m)) = m$:

- If $m_i = 0$ then $c_i \equiv x^2 \pmod{n}$, i.e., c_i is quadratic residue modulus $n = pq$.
  Then c_i is quadratic residue modulus p and $e_i = \left(\frac{c_i}{p}\right) = 1$, and, step 2 of the algorithm $m_i = 0$.
- If $m_i = 1$ then $c_i \equiv yx^2 \pmod{n}$. Given the fact that y is quadratic residue modulus n then c_i is also a quadratic residue modulus n.
  Then c_i is non-quadratic residue modulus $n = pq$, and we have that c_i is non-quadratic residue modulus p, so, $e_i = \left(\frac{c_i}{p}\right) = -1$, again by the step 2 of the algorithm we have, $m_i = 1$.

Having his/her private key A is able to easily compute $e_i = \left(\frac{c_i}{p}\right)$, and decrypt the message.

G-M Cipher — Security

Nota (G-M Cipher — Security)

Given the fact that x is randomly select from $\{1, 2, \ldots, n-1\}$:

- $x^2 \mod n$, *is a random quadratic residue modulus n.*
- $yx^2 \mod n$, *is a random pseudo-quadratic modulus n.*

Given $n = pq$, half of the elements $\left\{a \in \mathbb{N} : a \leq n \wedge \left(\frac{a}{n}\right) = 1\right\}$ are pseudo-quadratic modulus n, and the other half are quadratic residue modulus n

In conclusion, an adversary that menage to get access to the encrypted messages will have only access to random quadratic residues and pseudo-quadratic modulus n If the problem of the quadratic residues it is NP-complete, then the best the adversary can do is to try to get the right bits by pure chance between the elements of $m_1, m_2, \ldots, m_t$.

G-M Cipher — Example

Example: Goldwasser-Micali cipher with (very) small parameters

Keys generation

The entity A selects the primes $p = 499$ and $q = 547$, and computes $n = pq = 272953$.

He/she choose, $a \in \{1, 2, \ldots, 498\}$ such that $\left(\frac{a}{499}\right) = -1$.

e.g., $a = 236$

He/she choose, $b \in \{1, 2, \ldots 546\}$ such that $\left(\frac{b}{547}\right) = -1$.

e.g., $b = 378$;

G-M Cipher — Example

Keys generation (cont.)

He/she uses the Chinese remainder theorem to get $y \in \{1, 2, \ldots, n-1\}$ such that

$$\begin{cases} y \equiv 236 \pmod{499} \\ y \equiv 378 \pmod{547} \end{cases}.$$

We have $y = 55625$.

One of A's possible public keys is then: $(n, y) = (272953, 55625)$.

The A's private key is: $(p, q) = (499, 547)$.

G-M Cipher — Example

Encryption

B gets A's public key, $(n, y) = (272953, 55625)$ it represents the message $m = m_1 m_2 m_3 m_4 m_5 m_6 = 101110$, $(t = 6)$.

- $i = 1$, $x = 13349$, $m_1 = 1$ then $c_1 \leftarrow 55625 \cdot 13349^2 \mod 272953$, $c_1 = 84339$
- $i = 2$, $x = 1210$, $m_2 = 0$ then $c_2 \leftarrow 1210^2 \mod 272953$, $c_2 = 99335$
- $i = 3$, $x = 17839$, $m_3 = 1$ then $c_3 \leftarrow 55625 \cdot 17839^2 \mod 272953$, $c_3 = 134121$
- $i = 4$, $x = 5430$, $m_4 = 1$ then $c_4 \leftarrow 55625 \cdot 54309^2 \mod 272953$, $c_4 = 231199$

G-M Cipher — Example

Encryption (cont)

- $i = 5$, $x = 129$, $m_5 = 1$ then $c_5 \leftarrow 55625 \cdot 129^2 \mod 272953$, $c_5 = 72002$
- $i = 6$, $x = 2087$, $m_6 = 0$ then $c_6 \leftarrow 2087^2 \mod 272953$, $c_6 = 261274$

B sends $c = (84339, 99335, 134121, 231199, 72002, 261274)$ to A.

G-M Cipher — Example

Decryption

To decrypt c, A computes

- $e_1 = \left(\frac{84339}{499}\right) = -1$, then $m_1 \leftarrow 1$
- $e_2 = \left(\frac{99335}{499}\right) = 1$, then $m_2 \leftarrow 0$
- $e_3 = \left(\frac{134121}{499}\right) = -1$, then $m_3 \leftarrow 1$
- $e_4 = \left(\frac{231199}{499}\right) = -1$, then $m_4 \leftarrow 1$
- $e_5 = \left(\frac{72002}{499}\right) = -1$, then $m_5 \leftarrow 1$
- $e_6 = \left(\frac{261274}{499}\right) = 1$, then $m_6 \leftarrow 0$

The decrypt message is $m = m_1 m_2 \cdots m_6 = 101110$.

Pros & Cons of Public Key Ciphers

Pros

1. Only the private key should remain secret.
2. The keys can be kept for a long period.
3. The total number of keys is low.

Cons

1. The authenticity of the public keys must be certified.
2. Slow throughput
3. Length of the keys much larger then in the symmetric keys systems.
4. The security is based in non-proved assumptions.
5. With a still short, past history.

Stream Ciphers

In a stream cipher the plaintext digits are encrypted one at a time, and the transformation of successive digits varies during the encryption.

- It is possible to change the encryption function at each symbol;
- Do not suffer from error propagation problems;

Stream ciphers are often used in applications where plaintext comes in quantities of unknowable length - for example, a secure wireless connection.

Vernam Cipher

Definition (Vernam Cipher)

A Vernam cipher *it is a stream cipher defined in the alphabet* $\mathcal{A} = \{0, 1\}$. *One binary message* $m_1 m_2 \ldots m_t$ *is transformed through a stream key* $k_1 k_2 \ldots k_t$ *of the same length in order to produce* $c_1 c_2 \ldots c_t$, *where:*

$$c_i = m_i \oplus k_i, \quad 1 \leq i \leq t.$$

If the stream key is randomly generated and is never reused this cipher is designated as "one-time system" or "one-time pad".

- Claude Shannon, proved that the one-time pad is unbreakable in his World War II research that was later published in October 1949. It is the first and only encryption method for which there is such a proof.
- If the key is reused it is possible to break the cipher.