Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №4

з дисципліни

«Криптографія»

на тему: «Побудова генератора псевдовипадкових послідовностей на лінійних регістрах зсуву (генератора Джиффі) та його кореляційний криптоаналіз»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-74

Заіграєв Костянтин та Новіков Олексій

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О.

Мета роботи :

Ознайомлення з деякими принципами побудови криптосистем на лінійних регістрах зсуву; практичне освоєння програмної реалізації лінійних регістрів зсуву (ЛРЗ); ознайомлення з методом кореляційного аналізу криптосистем на прикладі генератора Джиффі.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. За даними характеристичними многочленами написати програму роботи ЛРЗ L1 , L2, L3 і побудованого на них генератора Джиффі.
2. За допомогою формул (4) – (6) при заданому α визначити кількість знаків вихідної послідовності N* , необхідну для знаходження вірного початкового заповнення, а також поріг C для регістрів L1 та L2 .
3. Організувати перебір всіх можливих початкових заповнень L1 і обчислення відповідних статистик R з використанням заданої послідовності (z_i) , i=0,N*-1
4. Відбракувати випробувані варіанти за критерієм R > C і знайти всі кандидати на істинне початкове заповнення L1 .
5. Аналогічним чином знайти кандидатів на початкове заповнення L2 .
6. Організувати перебір всіх початкових заповнень L3 та генерацію відповідних послідовностей (s_i) .
7. Відбракувати невірні початкові заповнення L3 за тактами, на яких $x_i != y_i$, де (x_i), (y_i) – послідовності, що генеруються регістрами L1 та L2 при знайдених початкових заповненнях.
8. Перевірити знайдені початкові заповнення ЛРЗ L1, L2 , L3 шляхом співставлення згенерованої послідовності (z_i) із заданою при i=0,N-1.

Вихідні дані:

Характеристичні многочлени:
– для L1 : $p(x) = x^{30} \oplus x^6 \oplus x^4 \oplus x \oplus 1$, що відповідає співвідношенню між членами послідовності $x_{i+30} = x_{i+6} \oplus x_{i+4} \oplus x_{i+1} \oplus x_i$;
– для L2 : $p(x) = x^{31} \oplus x^3 \oplus 1$, відповідна рекурента: $y_{i+31} = y_i \oplus y_{i+1}$;
– для L3 : $p(x) = x^{32} \oplus x^7 \oplus x^5 \oplus x^3 \oplus x^2 \oplus x \oplus 1$, відповідна рекурента: $s_{i+32} = s_i \oplus s_{i+1} \oplus s_{i+2} \oplus s_{i+3} \oplus s_{i+5} \oplus s_{i+7}$;
Імовірність помилки першого роду α = 0,01.

Результати

Знайдені критерії та довжини для регістрів:

LFSTR1: C = 81 N = 258

LFSTR2: C = 83 N = 265

Варіант 7

00011111001000001011011010001001110011001011100010110011111011110101001100110001010100010110101101101001011001010001000
00101100011101110000100100001111010101000010110000000011000101010111000011000000001101000011011101111100101000111101010
00110011101011001111101110111101110011010000101011100101101010100110010001010011010101111110111000101110011001001110010 1
01000000000100010010101100100000111010100011000011100010010010011001101000100101100011100001111100011000001001101011000
01001101010011000101100101110101011000110000110011000100001100000011111010010101010111110111001010010000111101100111001 1
01011001001011110000010000110010111011111011100000111110000010010100100010010101000011111111011100010110110101100010000
01011011111101010010000111001100000011001100011111010101000011001100010100000010000000100100011110010000111101110010110
11001110001110111111010001110101010001011100100110101110101000111001011011011110001010001110101011000101110100100110100
10101100010010100101101100000011100110110101001101000111011011100101100000001111001001011000100111110100101111101001 1
01110000000011110111001111000110011000011101100110010111010001110011111001101011110010111010001011001110110100100111001
10101011010100111111000101101111111000110001100110101000101101011100100101110110001010000111110010100001111110011110010 0
00111111101111110110100010001111110000111110000000011011011100111000101001010100110010000110011101101000111110101000010

100011110110011101101100011011111000100010101000010100111111110000110100111001100001111111011011000001000100010001000 11
1010011111100000011010111001010101101110011110101110101000100011101000100001101100010110110010001100001011000001001011 1
1101101001101110110000010101010010000110100110110000011001001010010001000001100111000010101001101111011001010001101100 1
1011100110111001110000111010100011011111111011111010100100000100111101110100100100111000001000111011101101100111011111 0
0001001011111110101010000001100100000101000011100001000111011111001011010011001100111111011010011100000101111000100010 1
001011110010010010110000 1

Початкові значення послідовностей:

L1: 001011111010010000000000011001100
L2: 000111111001000111011111010101000
L3: 110001100011001100001000101110 00

Повні послідовності:

L1 gamma:
001011111010010000000000011001101100011101011000011111011101101110101001110000001011010011110000001011001100
1111010111000000011000101001110011001001011110001010010101101110010010001010101110001011000100011110011010
0110111010000101010111100100111111101010001101100101011101010000010000101010100101100011100100010001110011
0101011110011110010111011101010110011011010000010011100100000111001001100111101001101010110010100100111011
0010101000010110100110001101010101101011110100000100010111001111110101011001011110000101011000010000100010
0001100000001111100011011000001101011100001011001011100110011100101101100100000001101000100001100101110111 11
0000010000001111000010001010000001001010010001110111011110011011101011011000110000011111111101010011010101 00
1000100010000000010101100101110011000110010000000001000000110001011111011001010011111100011011001110101100 1
1011101100101000001010000111111011010111110000111000001101101111111010010011100011010001011100111001101111 0
0000011100001001011111000000111011101111010011010001110100011000010110010000001101100001011101100111010110 1
0111110100101100000101011111111000111101011000000001111011011101100100110101100111100111011011010101100000 11
0110000100001101000110011010111111000010000000110110111111110011100110111010001011001111001011111111100111
1000011010000111000111101100010100001000111111011111100101110110101001101001111100000101011000000100101100 1
0000000000011000110101001110110000011110010001000010001111001001010111100001101010101010011001100001010010
1111110000010100111001011001111100000000100101000010000100100010101101111101100011100111100001010100111101 1
1101011000110001000111110001001001010100000101000101001000011010111000011011010101000100111001010101001101
1010101110100010111000011001101010111001110001010111011010101000100111010001010101101101010111001100110011
0010001101010001101010101011111000010010000001011111011101001111001010001011001011111011101001110111100100 0
1100101111101000000010111001110001100010111010010000100111101000110011111010011111111010000110010000110110
100100101001111110001010010110001 1

L2 gamma:
0001111110010001110111111010101001110011000111111001001011111100111101011111100110000010100110110101101001101 01
1001011001000000110001001001100100100100010011011100000001010000000001100010001111000101101000000110111001 11
1011110100010100011000111011010010101011011011101111111000010001111100000000110010001110100111100111000011 01
0001111101001101101111110110010111100101001000000010010001001010110011000010001000000110000111001010110100 110
0100110110111111001110001001010000100000001001101111111000011010100100010001000100011101100111000011001100 110
0111110001011111011010101010101100111101010010000111111111100101101011100001011100000000110010001101111010 1
0111100001101000111000101011110101110110010111111110111010101101100010010100000100110111100000111000011010
0100010001011100111111011001000011001101011101100010001000101101010011011000111001100110100011100100001111
1110101010010111111000101110000101111100010100011110101111010101001111011011110101101010111110011010000010
1011000111101001101001010010111001111101010010010001100010111011001011100000000111011101011000100101111000 0
1111001101100111000010101110111011010000101111101011101100110000101010101001011011000101011010111111110001
0000011101110001101000001111001001111001111110010100111011000011011011000110011001110001101100000000111101 0
1010111111100001100001110101111110100001110110110111101101000101010111100000000010100001011011111010111000 0
0101101010100001001011011110010100011111010100001000010110011011110010111010100101010010100010110010110111
0001111000110110100100100001111111011111000000100000000101110000100100111001001000010101111010000000111100000
0101011101010101000111011100010111011011111111011111001111101011000000100001001001101100101100110010010100 00
0010000100100101010000001101000100101000000001111010011001011000011010000111010100101001001101100101011110 11
1000110000010000100111010100111111011001001010001110111001100010001000001101111110011101011100110010011000 1
0011011101101110101000010111000100011000001101110101010111110011101100110001101111110100110111000101011110
001000101001000111110111010111100 1

L3 gamma:
1100011000110011000010001011100010111100111001000011010110100111001111111000000001010000100011010000100101 10
0001011000000111011101110100110110001010011110101011000111111000100101101011111100101100101110110110111000 01
0111011010000001000011011001110000110010011010000011000110101010011101010100011111111100101110000111010111 11
0101110110011101111010100010001100000000101110110100100100001000110011000011011100010010000000111001100001 0
1011010101111110101001001010101001011000010010101001101001100010011001111011111101101001010000110010001110 0
1111011011101001001010100101010011011110011001101110010111111100000101111010100111010111100111011111110101 1
0000101010011101111110000000101101011111000111100001000010101110000010010110000010110100111111111111010010110
1010010010010000100101001101001010000000100101111101110111011100100111100100110010101010001011111100011001 0
0001001010101101010101000100010111101011001010001010010110111111000111001110110000011110100010000101101001 1
0100000111000110111010010110101000010000110011100100110100001100100010101111011010101100100101111100011011
1101111111101001000010110000100111101001011100111000110010111011010000100111000100001000001100111010101001

11101001100110101001110111011011001011100000110001101001001010100111110111111111110011011110101110111100000111001100011001100110010110000100001000011111111001100110001010010010101011110111110100100010011010100110011010101111100001000011101110000110000000000010011111001101011000100001011011010110000101000111011011001111101011010000001001000001001100001101101001110101011100000110001010100000111101111110111001111000000000011100101000110111010100001101011101111010011111000100010111001101110001010011110110101000010101010010110011110000111011000011000101000111001111100111101110010111100101001011101000000111011000101000000010111010101110010001010011100101010111011010011110010011110010111010010100111000111111001111001101101001000011001111011010011010111100001010010011101101100110101000100001011000100110100000010011011100000100010101010011010111110011111001111011

Код програми

```
#include "compute.cuh"

#include <bitset>//num to bin for answer
#pragma comment (lib, "cudart64_102.dll")


using namespace std;


double getBeta(pPolynom poly, double percent) {
	double Border = double(1) / pow(2, poly->polynom[0]);
	return Border * percent;
}

void getParams(pPolynom poly, pcrackParams params, int *C, int *Ns) {
	boost::math::normal dist(0.0, 1.0);
	double beta = getBeta(poly, params->betaPercent);
	double QuantileAlpha = quantile(dist, 1 - params->alpha);
	double QuantileBeta  = quantile(dist, 1 - beta);
	double NsDouble = pow((QuantileBeta + ((QuantileAlpha * sqrt(params->p1 * (1 - params->p1))) / sqrt(params->p2 * (1 - params->p2)))) * (sqrt(params->p2 * (1 - params->p2)) / (params->p2 - params->p1)), 2);
	*C = (NsDouble * params->p1 + QuantileAlpha * sqrt(NsDouble * params->p1 * (1 - params->p1))) + 1;
	*Ns = NsDouble + 1;
}


double getCuda_optimalSize(pPolynom poly, int Ns, int z_size) {
	int maxBlocks, maxThreads;
	unsigned long long memoryByte, mem_per_thread, mem_shared, mem_total;

	mem_per_thread = 2048 * sizeof(unsigned int) + 2 * 64 * sizeof(unsigned int) + sizeof(unsigned char) + 3 * sizeof(unsigned int) + 10 * sizeof(int) + 32 * sizeof(unsigned int);

			//poly2->polynom = new unsigned int[3]{ 31, 3, 0 };
	//poly2->size = 3;
	poly2->polynom = new unsigned int[5]{ 26, 6, 2, 1, 0 };
	poly2->size = 5;
	pPolynom poly3 = new Polynom;
	//poly3->polynom = new unsigned int[7]{ 32, 7, 5, 3, 2, 1, 0 };
	//poly3->size = 7;
	poly3->polynom = new unsigned int[5]{ 27, 5, 2, 1, 0 };
	poly3->size = 5;
	vector<unsigned int> L1_probable, L2_probable, result;
	plfstrHistory lfstr1_init = new lfstrHistory;
	plfstrHistory lfstr2_init = new lfstrHistory;

	int NsInt, C;
	getParams(poly1, params, &C, &NsInt);

	lfstr1_init->parts = unsigned int(getCuda_optimalSize(poly1, NsInt, C));

	unsigned int period;

	cout << "LFSTR1" << endl;
	cout << "CPU calculation of init vectors for CUDA parallelism" << endl;
	lfstr(1, poly1, &period, lfstr1_init);

	cuda_lfstrCrack(lfstr1_init, poly1, z, NsInt, C, &L1_probable);
	cout << "Num of probable vectors: " << L1_probable.size() << endl;
	/*
	for (int i = 0; i < L1_probable.size();i++) {
			cout << L1_probable[i] << endl;
	}
	*/
	mem_shared = 40000 * sizeof(unsigned int) + 64 * sizeof(unsigned int) + poly->size * sizeof(unsigned int) + sizeof(unsigned int) + 100 * sizeof(unsigned int);
	mem_total = mem_per_thread + mem_shared;

	cudaDeviceProp deviceProp;
	cudaGetDeviceProperties(&deviceProp, 0);
	cout << "Found: " << deviceProp.name << endl;
	maxBlocks = deviceProp.maxGridSize[0];
	maxThreads = deviceProp.maxThreadsDim[0];
	memoryByte = deviceProp.totalGlobalMem;
	//memoryByte -= pow(2, 28);
	memoryByte = (double)(memoryByte) * 0.9;
	memoryByte -= mem_shared;


	return ((double)(memoryByte / mem_per_thread)) * 0.95;
}


int main() {
	vector <unsigned int> z;
	//int N = getZ("test_big", &z);
	int N = getZ("test_small", &z);
	pcrackParams params = new crackParams;
	params->alpha = 0.01;
	params->p1 = 0.25;
	params->p2 = 0.5;
	params->betaPercent = 0.99;

	pPolynom poly1 = new Polynom;
	//poly1->polynom = new unsigned int[5]{ 30, 6, 4, 1, 0 };
	//poly1->size = 5;
	poly1->polynom = new unsigned int[3]{ 25, 3, 0 };
	poly1->size = 3;
	pPolynom poly2 = new Polynom;

	system("pause");

	return 0;
}


int getZ(string file, vector <unsigned int>* z)
{
	fstream zFile;
	char* read = new char[1];
	zFile.open(file, ios::in | ios::binary | ios::ate);
	streampos fileLen = zFile.tellg();
	zFile.seekg(0, ios::beg);
	for (int i = 0; i < fileLen; i++)
	{
		if (i % 32 == 0)
			z->push_back(0);
		zFile >> read[0];
		(*z)[i / 32] |= (int(read[0]) - 48) << (31 - (i % 32));
	}
	delete[] read;
	zFile.close();
	return fileLen;
}



void lfstr(unsigned int init, pPolynom polynom, unsigned int* period, plfstrHistory history) {
	unsigned char new_bit;
	unsigned int curr = init;
	unsigned int bit_length = polynom->polynom[0];
	*period = 0;
	unsigned int max_iters = (1 << polynom->polynom[0]) - 1;
	if (polynom->polynom[0] == 32)
		max_iters = 4294967295;
	unsigned int modulo;
	//cout << max_iters << endl;
```

```
	cout << "LFSTR2" << endl;
	cout << "CPU calculation of init vectors for CUDA parallelism" << endl;
	getParams(poly2, params, &C, &NsInt);
	lfstr2_init->parts = unsigned int(getCuda_optimalSize(poly2, NsInt, C));
	lfstr(1, poly2, &period, lfstr2_init);
	cuda_lfstrCrack(lfstr2_init, poly2, z, NsInt, C, &L2_probable);

	cout << "Num of probable vectors: " << L2_probable.size() << endl;
	/*for (int i = 0; i < L2_probable.size(); i++) {
		//cout << L2_probable[i] << endl;
	}*/



	cout << "LFSTR3" << endl;


	cout << "CPU preparations for CUDA" << endl;

	cuda_GeffeCrack(poly1, poly2, poly3, z, L1_probable, L2_probable, &result);


	cout << "\n---------------------------------------------------------- \nRESULT:" << endl;

	for (int i = 0; i < result.size(); i++) {
		string bits = std::bitset<32>(result[i]).to_string();
		reverse(bits.begin(), bits.end());
		cout << "L" << i+1 << ": " << bits << endl;
	}

	cout << "L1 gamma:" << endl;
	vector<unsigned int> arr = get_lfstr_res(result[0], poly1);
	for (int i = 0; i < arr.size(); i++)
		cout << std::bitset<32>(arr[i]).to_string();
	cout << "\n" << endl;

	cout << "L2 gamma:" << endl;
	arr = get_lfstr_res(result[1], poly2);
	for (int i = 0; i < arr.size(); i++)
		cout << std::bitset<32>(arr[i]).to_string();
	cout << "\n" << endl;

	cout << "L3 gamma:" << endl;
	arr = get_lfstr_res(result[2], poly3);
	for (int i = 0; i < arr.size(); i++)
		cout << std::bitset<32>(arr[i]).to_string();
	cout << "\n" << endl;

	cout << "EO CRACKING!" << endl;

		R = 0;

		for (int i = 1; i < polynom->size; i++) {
			new_bit ^= (curr & (1 << polynom->polynom[i])) >> polynom->polynom[i];
		}


		temp_bit = (x[vectorSize - 1] & (1 << 31)) >> 31;
		x[vectorSize - 1] <<= 1;
		x[vectorSize - 1] |= curr & 1;
		for (int i = vectorSize-2; i >= 0; i--) {
			temp_bit2 = (x[i] & (1 << 31)) >> 31;
			x[i] <<= 1;
			x[i] |= temp_bit;
			temp_bit = temp_bit2;
		}


		if (history.size() == Ns-1) {
			for (int i = 0; i < Ns; i++) {
				R += ((z[i / 32] & (1 << (31 - (i % 32)))) >> (31 - (i % 32))) ^ ((x[(2048 - Ns + i) / 32] & (1 << (31 - ((2048 - Ns + i) % 32)))) >> (31 - ((2048 - Ns + i) % 32)));
			}
			if (R < C) {
				probable->push_back(history[0]);
			}
			history.erase(history.begin());
		}
		history.push_back(curr);


		curr >>= 1;
		curr |= new_bit << (bit_length - 1);

		/*
		if (final_Countdown) {
	if (history != nullptr) {
		if (history->parts == 0)
			modulo = 1;
		else
			modulo = max_iters / history->parts;
	}

	while (true) {
		new_bit = 0;

		if (history != nullptr && *period % modulo == 0)
			history->history.push_back(curr);

		*period += 1;

		for (int i = 1; i < polynom->size; i++) {
			new_bit ^= (curr & (1 << polynom->polynom[i])) >> polynom->polynom[i];
		}

		curr >>= 1;
		curr |= new_bit << (bit_length - 1);

		if (curr == init || *period >= max_iters) {
			if (history != nullptr)
				history->size = history->history.size();
			return;
		}
	}
}



void lfstr_Crack_old(unsigned int init, pPolynom polynom, vector <unsigned int> z, int Ns, int C, vector <unsigned int>* probable) {
	unsigned char new_bit, temp_bit, temp_bit2;
	unsigned int curr = init;
	unsigned int bit_length = polynom->polynom[0];
	int* final_Countdown=nullptr;

	unsigned int max_iters = (1 << polynom->polynom[0]) - 1;
	cout << max_iters << endl;

	vector<unsigned int> history, x = z;
	int vectorSize = x.size();

	int R;
	for (int iter = 0; iter < max_iters + Ns; iter++) {
		if (iter % 10000000 == 0)
			cout << iter << endl;


		new_bit = 0;
			return;
		printf("%d) %d\n", iter, curr);*/

		/*
		if (iter == 15648) {
			for (unsigned int i = 0; i < vectorSize; i++) {
				printf("%d) \t%d\n", i, x[i]);
			}
			return;
		}
		*/

		if (history.size() == Ns - 1) {
			for (int i = 0; i < Ns; i++) {
				R += ((z[i / 32] & (1 << (31 - (i % 32)))) >> (31 - (i % 32))) ^ ((x[(2048 - Ns + i) / 32] & (1 << (31 - ((2048 - Ns + i) % 32)))) >> (31 - ((2048 - Ns + i) % 32)));
			}
			if (R < C) {
				probable->push_back(history[0]);
			}
			history.erase(history.begin());
		}
		history.push_back(curr);


		curr >>= 1;
		curr |= new_bit << (bit_length - 1);

	}
	history.clear();
	history.shrink_to_fit();
	x.clear();
	x.shrink_to_fit();
	z.clear();
	z.shrink_to_fit();
}
```

```
                                        *final_Countdown--;
                                        if (*final_Countdown == 0)
                                                return;
                                }

                                if (curr == init) {
                                        final_Countdown = new int(Ns);
                                }
                                */
                        }
}


void lfstr_Crack(unsigned int init, pPolynom polynom, vector <unsigned int> z,
int Ns, int C, vector <unsigned int>* probable) {
                unsigned char new_bit, temp_bit, temp_bit2;
                unsigned int curr = init;
                unsigned int bit_length = polynom->polynom[0];

                unsigned int max_iters = (1 << polynom->polynom[0]) - 1;
                cout << max_iters << endl;

                vector<unsigned int> history, x = z;
                int vectorSize = x.size();
                for (int i = 0; i < x.size(); i++)
                        x[i] = 0;

                int R;
                for (int iter = 0; iter < max_iters + Ns; iter++) {
                        if (iter % 10000000 == 0)
                                cout << iter << endl;



                        new_bit = 0;
                        R = 0;

                        for (int i = 1; i < polynom->size; i++) {
                                new_bit ^= (curr & (1 << polynom-
>polynom[i])) >> polynom->polynom[i];
                        }


                        temp_bit = (x[vectorSize - 1] & (1 << 31)) >> 31;
                        x[vectorSize - 1] <<= 1;
                        x[vectorSize - 1] |= curr & 1;
                        for (int i = vectorSize - 2; i >= 0; i--) {
                                temp_bit2 = (x[i] & (1 << 31)) >> 31;
                                x[i] <<= 1;
                                x[i] |= temp_bit;
                                temp_bit = temp_bit2;
                        }

                        /*
                        if (iter == 1489)
void cuda_GeffeCrack(pPolynom polynom1, pPolynom polynom2, pPolynom
polynom3, vector <unsigned int> z, vector <unsigned int> lfstr1, vector
<unsigned int> lfstr2, vector<unsigned int>* result) {
                //unsigned int z;
                vector<unsigned int> lfstr1_res, lfstr2_res, polynom_vector, temp,
temp2, pairs, cudaRes, arr;
                vector<vector<unsigned int>> polynoms;
                unsigned int known_mask, unknown_mask, known_z, possible = 0;
                for (int i = 0; i < polynom1->size; i++)
                        polynom_vector.push_back(polynom1->polynom[i]);
                polynoms.push_back(polynom_vector);
                polynom_vector.clear();
                for (int i = 0; i < polynom2->size; i++)
                        polynom_vector.push_back(polynom2->polynom[i]);
                polynoms.push_back(polynom_vector);
                polynom_vector.clear();
                for (int i = 0; i < polynom3->size; i++)
                        polynom_vector.push_back(polynom3->polynom[i]);
                polynoms.push_back(polynom_vector);
                polynom_vector.clear();
                /*
                for (int i = 0; i < lfstr1.size(); i++) {
                        temp = get_lfstr_res(lfstr1[i], polynom1);
                        for (int j = 0; j < temp.size(); j++)
                                lfstr1_res.push_back(temp[j]);
                }
                for (int i = 0; i < lfstr2.size(); i++) {
                        temp = get_lfstr_res(lfstr2[i], polynom2);
                        for (int j = 0; j < temp.size(); j++)
                                lfstr2_res.push_back(temp[j]);
                        kernel_crackGeffe(init_arr, polynom_vector, z,
lfstr1_res, lfstr2_res, &cudaRes);
                        lfstr2_res.clear();
                        cudaRes.clear();
                        cout << i << endl;
                        if (cudaRes[2] != 0)
                                break;
                }
```

```
void cuda_lfstrCrack(plfstrHistory init_arr, pPolynom polynom, vector <unsigned
int> z, int Ns, int C, vector<unsigned int>* probable) {
                vector<unsigned int> polynom_vector;
                for (int i = 0; i < polynom->size; i++)
                        polynom_vector.push_back(polynom->polynom[i]);

                kernel_crackLFSTR(init_arr, polynom_vector, z, Ns, C, probable);
                polynom_vector.clear();
                polynom_vector.shrink_to_fit();
                init_arr->history.clear();
                init_arr->history.shrink_to_fit();
                delete init_arr;
                sort(probable->begin(), probable->end());
                probable->erase(unique(probable->begin(), probable->end()),
probable->end());
}


vector <unsigned int> get_lfstr_res(unsigned int init, pPolynom polynom, int
iterations) {
                unsigned char new_bit, temp_bit, temp_bit2;
                unsigned int curr = init;
                unsigned int bit_length = polynom->polynom[0];
                int vector_size;
                if (iterations % 32 == 0)
                        vector_size = iterations / 32;
                else
                        vector_size = (iterations / 32) + 1;
                vector<unsigned int> res(vector_size);

                for (int iter = 0; iter < iterations; iter++) {
                        new_bit = 0;

                        for (int i = 1; i < polynom->size; i++) {
                                new_bit ^= (curr & (1 << polynom-
>polynom[i])) >> polynom->polynom[i];
                        }

                        temp_bit = (res[vector_size - 1] & (1 << 31)) >> 31;
                        res[vector_size - 1] <<= 1;
                        res[vector_size - 1] |= curr & 1;
                        for (int i = vector_size - 2; i >= 0; i--) {
                                temp_bit2 = (res[i] & (1 << 31)) >> 31;
                                res[i] <<= 1;
                                res[i] |= temp_bit;
                                temp_bit = temp_bit2;
                        }

                        curr >>= 1;
                        curr |= new_bit << (bit_length - 1);

                }
                return res;
}
//                                      cout << "Possible" << possible++ << ": "
<< lfstr1[i] << " " << lfstr2[j] << endl;
                                        arr.push_back(lfstr1[i]);
                                        temp2.push_back(lfstr2[j]);
                                        pairs.push_back(i * lfstr2.size() + j);
                                        //known_z |= (lfstr1_local[0] &
known_mask) ^ (~(z_local[0] & known_mask));
                                }
                        }



                sort(arr.begin(), arr.end());
                arr.erase(unique(arr.begin(), arr.end()), arr.end());
                temp = arr;
                sort(temp2.begin(), temp2.end());
                temp2.erase(unique(temp2.begin(), temp2.end()), temp2.end());

                for (int i = 0; i < pairs.size(); i++) {
                        int index_l1 = pairs[i] / lfstr2.size();
                        int index_l2 = pairs[i] % lfstr2.size();
                        for (int j = 0; j < temp.size(); j++) {
                                if (lfstr1[index_l1] == temp[j]) {
                                        index_l1 = j;
                                        break;
                                }
                        }
                        for (int j = 0; j < temp2.size(); j++) {
                                if (lfstr2[index_l2] == temp2[j]) {
                                        index_l2 = j;
                                        break;
                                }
                        }
                        pairs[i] = index_l1 * temp2.size() + index_l2;
                }
                lfstr1 = temp;
                lfstr2 = temp2;
                temp2.clear();
                temp2.shrink_to_fit();
```

```
		known_mask = lfstr1_local[0] ^ lfstr2_local[0];

		if (lfstr1_local[0] & ~known_mask != z_local[0] & ~known_mask)
			return;

		known_z |= (lfstr1_local[0] & known_mask) ^ (~(z_local[0] &
known_mask));


		for (int i = 0; i < lfstr1.size(); i++) {
			vector<unsigned int>t1 = get_lfstr_res(lfstr1[i],
polynom1, 2048);
			for (int j = 0; j < lfstr2.size(); j++) {
				vector<unsigned int>t2 =
get_lfstr_res(lfstr2[i], polynom2, 2048);
				bool tr = true;
				for (int k = 0; k < 2048; k++) {
					known_mask = t1[i] ^ t2[j];

					if ((t1[i] & ~known_mask) !=
(z[0] & ~known_mask)) {
						tr = false;
						break;
					}
				}
				if (tr == true) {
					cout << "Possible" <<
possible++ << ": " << lfstr1[i] << " " << lfstr2[j] << endl;
					temp1.push_back(lfstr1[i]);
					temp2.push_back(lfstr2[i]);
					pairs.push_back(i *
lfstr2.size() + j);
				}
				//known_z |= (lfstr1_local[0] &
known_mask) ^ (~(z_local[0] & known_mask));
			}
		}

		*/

		unsigned int z_rev;
		//temp1.empty();
		z_rev = reverseBits(z[0]);//get_lfstr_res(z[0], polynom1, 32);
		unsigned int end_mask = pow(2, min(polynoms[0][0],
polynoms[1][0], polynoms[2][0])) - 1;

		for (int i = 0; i < lfstr1.size(); i++) {
			for (int j = 0; j < lfstr2.size(); j++) {
				known_mask = lfstr1[i] ^ lfstr2[j];
				unknown_mask = ~known_mask;
				unknown_mask &= end_mask;

				if ((lfstr1[i] & unknown_mask) != (z_rev &
unknown_mask))
					continue;
```

```
		for (int i = 0; i < lfstr1.size(); i++) {
			temp = get_lfstr_res(lfstr1[i], polynom1);
			for (int j = 0; j < temp.size(); j++)
				lfstr1_res.push_back(temp[j]);
		}

		for (int i = 0; i < lfstr2.size(); i++) {
			temp = get_lfstr_res(lfstr2[i], polynom2);
			for (int j = 0; j < temp.size(); j++)
				lfstr2_res.push_back(temp[j]);
		}
		temp.clear();
		temp.shrink_to_fit();
		cout << "Number of probable pairs: "<< pairs.size() << endl;
		unsigned int* cudaPointer = kernel_crackGeffe(polynoms[2],
min(polynoms[0][0], polynoms[1][0], polynoms[2][0]), z, lfstr1_res, lfstr2_res,
pairs);
		cudaRes.assign(cudaPointer, cudaPointer + 3);
		free(cudaPointer);
		polynom_vector.clear();
		polynom_vector.shrink_to_fit();
		result->push_back(lfstr1[cudaRes[0]]);
		result->push_back(lfstr2[cudaRes[1]]);
		result->push_back(cudaRes[2]);
}


unsigned int reverseBits(unsigned int num)
{
		unsigned int count = sizeof(num) * 8 - 1;
		unsigned int reverse_num = num;

		num >>= 1;
		while (num)
		{
			reverse_num <<= 1;
			reverse_num |= num & 1;
			num >>= 1;
			count--;
		}
		reverse_num <<= count;
		return reverse_num;
}
```

Висновки:

Під час данного комп’ютерного практикуму, ми ознайомились з деякими принципами побудови криптосистем на лінійних регістрах зсуву та з методом кореляційного аналізу криптосистем на прикладі генератора Джиффі.