MAMME FME

Codes and Cryptography

Final Exam 9 January 2015

Options: (Select one)

☐ **Only Coding** (only if you passed the Cryptography partial exam):
— Solve **all** the exercises in the Coding Theory part

☐ **Only Crypto** (only if you passed the Coding Theory partial exam):
— Solve **all** the exercises in the Cryptography part

☐ **Both parts**:
Solve the items **marked with** *** in both parts

Coding Theory Part

*** 1. Consider the following family of binary codes $\mathcal{C}_{x,y} = \{0110, 01011, 101, xy\}$, for $x, y \in \{0, 1\}$. Determine which choices for x and y make the code uniquely decodable. Determine also which ones are prefix-free.

2. Given a non-uniform source with symbol probabilities

$$\mathcal{S} = (1/20, 5/20, 3/20, 2/20, 3/20, 4/20, 2/20)$$

build a binary Huffman code for it, and compute the corresponding average word length.

*** 3. Build a generating matrix of the 5-ary Hamming code of length 6. Give its dimension and minimum distance. Show also that it is perfect and MDS.

4. Build the generating matrix of a 7-ary cyclic code of length 8 and dimension 5. To that end, consider the following splitting into irreducible factors in $\mathbb{F}_7[X]$

$$X^8 - 1 = (X - 1)(X + 1)(X^2 + 1)(X^2 + 3X + 1)(X^2 - 3X + 1)$$

What can be deduced for this code from Singleton's bound?

By means of its dual code, build also a parity check matrix.

Cryptography Part

*** 1. Given a function family $\mathcal{F} = \{f_k : X_k \to Y_k\}_{k \in \mathcal{K}}$, define the following family of extended functions $\widehat{\mathcal{F}} = \{\widehat{f}_k : X_k \times X_k \to Y_k \times X_k\}_{k \in \mathcal{K}}$ such that $\widehat{f}_k(x, u) = (f_k(x), x \oplus u)$, where $\oplus$ denotes some (efficiently computable) group operation on X_k. Prove that $\mathcal{F}$ is one-way if and only $\widehat{\mathcal{F}}$ is one-way.

2. Catalano's public key encryption scheme is a variant of Paillier's that is more efficient but loses its homomorphic properties. The key generation is the same as in RSA, but the encryption function is $\text{Enc}(m) = r^e(1 + mn) \bmod n^2$, where $0 < r < n$ is a random integer and (n, e) is the public key.

   (a) Write in details the key generation procedure of RSA.

   (b) Design a decryption procedure, based on recovering the randomness r by means of the RSA decryption function.

   (c) Show that this encryption scheme does not have the homomorphic properties of Paillier's scheme.

*** 3. Consider the FDH-RSA signature scheme, with public key (N, e, H). Suppose a user P secretly obtains a valid signature σ on a public message m.

   (a) Give a 3-moves zero-knowledge proof of knowledge protocol where P proves knowledge of a valid FDH-RSA signature σ on public message m, for the public key (N, e, H), without revealing anything else on σ. Show the security properties of this zero-knowledge protocol. [**Hint:** σ is a pre-image of $H(m)$ for the homomorphic RSA permutation $f_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ defined by $f_e(x) = x^e \mod N$.]

   (b) Use the previous protocol to derive (via the Fiat-Shamir heuristic) an identity-based signature scheme, where the master entity knows the FDH-RSA secret key, and the secret key for a user with identity id is a FDH-RSA signature on the message $m = \text{id}$.

4. An access structure $\Gamma \subset 2^{\mathcal{P}}$ defined on a set of players $\mathcal{P} = \{P_1, \ldots, P_n\}$ is said to be *weighted threshold* if there exist positive integers $T, w_1, \ldots, w_n \in \mathbb{Z}^+$ such that, for any subset of players $A \subset \mathcal{P}$, we have $A \in \Gamma \Leftrightarrow \sum_{P_i \in A} w_i \geq T$.

   (a) Give a generalization of Shamir's threshold secret sharing scheme that works for a weighted threshold structure Γ. What is the information rate of the scheme ?

   (b) Prove that the access structure Γ defined by the basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}, \{P_1, P_4\}\}$, on a set of 4 players, is **not** weighted threshold.

   (c) Prove that the access structure Γ defined by the basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_4\}, \{P_2, P_4\}, \{P_3, P_4\}, \{P_4, P_5\}\}$, on a set of 5 players, **is** weighted threshold, and can be realized with a scheme with information rate $1/3$.

4/4/415 → 4.3

MAMME FME

Codes and Cryptography

Final Exam — 9 January 2015

Options: (Select one)

☐ **Only Coding** (only if you passed the Cryptography partial exam):
— Solve **all** the exercises in the Coding Theory part

☒ **Only Crypto** (only if you passed the Coding Theory partial exam):
— Solve **all** the exercises in the Cryptography part

☐ **Both parts**:
— Solve the items **marked with** *** in both parts

Coding Theory Part

*** 1. Consider the following family of binary codes $\mathcal{C}_{x,y} = \{0110, 01011, 101, xy\}$, for $x, y \in \{0, 1\}$. Determine which choices for x and y make the code uniquely decodable. Determine also which ones are prefix-free.

2. Given a non-uniform source with symbol probabilities

$$\mathcal{S} = (1/20, 5/20, 3/20, 2/20, 3/20, 4/20, 2/20)$$

build a binary Huffman code for it, and compute the corresponding average word length.

*** 3. Build a generating matrix of the 5-ary Hamming code of length 6. Give its dimension and minimum distance. Show also that it is perfect and MDS.

4. Build the generating matrix of a 7-ary cyclic code of length 8 and dimension 5. To that end, consider the following splitting into irreducible factors in $\mathbb{F}_7[X]$

$$X^8 - 1 = (X - 1)(X + 1)(X^2 + 1)(X^2 + 3X + 1)(X^2 - 3X + 1)$$

What can be deduced for this code from Singleton's bound?

By means of its dual code, build also a parity check matrix.

Cryptography Part

*** 1. Given a function family $\mathcal{F} = \{f_k : X_k \to Y_k\}_{k \in \mathcal{K}}$, define the following family of extended functions $\widehat{\mathcal{F}} = \{\widehat{f_k} : X_k \times X_k \to Y_k \times X_k\}_{k \in \mathcal{K}}$ such that $\widehat{f_k}(x, u) = (f_k(x), x \oplus u)$, where $\oplus$ denotes some (efficiently computable) group operation on X_k. Prove that $\mathcal{F}$ is one-way if and only $\widehat{\mathcal{F}}$ is one-way.

2. Catalano's public key encryption scheme is a variant of Paillier's that is more efficient but loses its homomorphic properties. The key generation is the same as in RSA, but the encryption function is $\text{Enc}(m) = r^e(1 + mn) \bmod n^2$, where $0 < r < n$ is a random integer and (n, e) is the public key.

   (a) Write in details the key generation procedure of RSA.

   (b) Design a decryption procedure, based on recovering the randomness r by means of the RSA decryption function.

   (c) Show that this encryption scheme does not have the homomorphic properties of Paillier's scheme.

*** 3. Consider the FDH-RSA signature scheme, with public key (N, e, H). Suppose a user P secretly obtains a valid signature σ on a public message m.

   (a) Give a 3-moves zero-knowledge proof of knowledge protocol where P proves knowledge of a valid FDH-RSA signature σ on public message m, for the public key (N, e, H), without revealing anything else on σ. Show the security properties of this zero-knowledge protocol. [**Hint:** σ is a pre-image of $H(m)$ for the homomorphic RSA permutation $f_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ defined by $f_e(x) = x^e \mod N$.]

   (b) Use the previous protocol to derive (via the Fiat-Shamir heuristic) an identity-based signature scheme, where the master entity knows the FDH-RSA secret key, and the secret key for a user with identity id is a FDH-RSA signature on the message $m = \text{id}$.

4. An access structure $\Gamma \subset 2^{\mathcal{P}}$ defined on a set of players $\mathcal{P} = \{P_1, \ldots, P_n\}$ is said to be *weighted threshold* if there exist positive integers $T, w_1, \ldots, w_n \in \mathbb{Z}^+$ such that, for any subset of players $A \subset \mathcal{P}$, we have $A \in \Gamma \Leftrightarrow \sum_{P_i \in A} w_i \geq T$.

   (a) Give a generalization of Shamir's threshold secret sharing scheme that works for a weighted threshold structure Γ. What is the information rate of the scheme ?

   (b) Prove that the access structure Γ defined by the basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}, \{P_1, P_4\}\}$, on a set of 4 players, is **not** weighted threshold.

   (c) Prove that the access structure Γ defined by the basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_4\}, \{P_2, P_4\}, \{P_2, P_4\}, \{P_4, P_5\}\}$, on a set of 5 players, is weighted threshold, and can be realized with a scheme with information rate 1/3.

(1) To prove: $\nexists$ OW $\Rightarrow$ $\nexists$ OW

✓ $\Leftrightarrow$ $\neg f$ OW $\Rightarrow \neg \hat{f}$ OW.

$\Rightarrow$ If f is not OW, then $\exists A_f$ s.t.

$$Pr[A_f(f_n(x)) \in f^{-1}(f(x)),\ x \in X_n] > \varepsilon,$$

but then $Pr[B_{\hat{f}}(\hat{f}_n(x)) \in \hat{f}^{-1}(\hat{f}(x,u)),\ x \in X_n, u \in Y_n]$

$= Pr[B_{\hat{f}}(\hat{f}_n(x)) \in (\hat{f}^{-1}(f(x)), x \oplus u),\ x \in X_n, u \in Y_n]$

$\geq_m \varepsilon$, because $f^{-1}(x)$ is not OW.

Not a correct proof !!!

$\Leftarrow$?

4

(2) a) Let $N = p \cdot q$, where p and q are 2 different 512-bit long primes.

and $e \geq 3$ $\in GR^{\mathbb{Z}}_N$ coprime with

$\phi(n) = (p-1)(q-1)$, i.e. $\gcd(e, \phi(N)) = 1$.

Key generation:

KeyGen(R): ~~& Comp~~

Input: p, q, e

Compute: $d = e^{-1} \bmod \text{lcm}(p-1, q-1)$

Output: Public key (n), e, private key ~~d~~ (p, q, ?)

✓

b)

b) $Dec(c) = \frac{c \cdot r^d - 1}{n} = m$, because $d = e^{-1} \bmod N$. in RSA.

r is unknown !!!

Recovering r ?

different r's

(2) c) $Enc(m_1) \cdot Enc(m_2)$

$= [r^e (1+m_1 n) \bmod n^2] \cdot [r^e (1+m_2 n) \bmod n^2]$

$= [r^e (1+m_1 n) \cdot r^e (1+m_2 n)] \bmod n^2$

$= [r^{2e} (1 + m_1 n + m_2 n + m_1 m_2 n^2)] \bmod n^2$

$= [r^{2e} (1 + m_1 n + m_2 n) \bmod n^2$

$Enc(m_1+m_2) = [r^e (1 + m_1 n + m_2 n)] \bmod n^2$

$Enc(m_1) \cdot Enc(m_2) \neq Enc(m_1 + m_2)$.

Not a correct proof !!!

(3) a)

~~1)~~ (P) ~~chooses~~ $\phi(N)$ secret!!! not known by P...

1) (P) sends N, $H(m)$, $\in \mathbb{Z}_p$ to (V)

2) (V) ~~computes e, s.t.~~ chooses $e \in_R \mathbb{Z}_p$, s.t. $\gcd(e, \phi(N)) = 1$ and sends e to (P)

e is fixed and public!!

3) (P) computes $\sigma^e = R$ and sends R to (V)

4) (V) outputs 1 iff $H(m) \bmod N = R$.

Security properties:

Completeness: Trivial

PoK: Extractor runs (P) until step 3, with random e and obtains $R = \omega^e$.

Then he rewinds back to step 2, chooses a different $e' \neq e$ and lets (P) output R'.

The extracted witness $x = (R \cdot R')^{-(e+e')}$

fulfills $x = H(m) \bmod N$. and what ?

ZK: A transcript ~~of the~~ $(R, e, H(m), N, \phi(N))$ ~~can be~~ of the protocol between P and V' can be simulated by S as follows:

(1) Choose $R \in_R \mathbb{Z}_p$

(2) Choose $e \in_R \mathbb{Z}_p$ ~~$\neq 2$~~ s.t. $\gcd(e, \phi(N)) = 1$ with the same distribution as V' does.

(3) Compute $\omega = R^{-e}$.

$\omega^e = R$, as in your protocol !!

(3) b) ID-Based signature:

1) Master key Generation: Compute secret key d and public key (N, e, H) as before in (3) a).

2) User key generation:

Master entity generates $\sigma_i = H(id_i)^d \bmod N$ and gives ~~secret~~ secret key σ_i to user i. ✓

3) Signature: User i signs messages m^* as $\sigma' = H(m^*)^{\sigma_i} \bmod N$ and defines the final signature as $\sigma = ((N, e, H(\cdot)), \sigma_i, \sigma')$

NO !! don't include secret key σ_i into a public signature !!

4) Verification: Output $Vfy(\sigma_i, \underbrace{m^*}_{id_i}) \wedge Vfy(\sigma', m^*)$

how ?

(4) a) General Shamir's threshold SSS. (t, n)

1) Dealer chooses n distinct, non-zero elements of $\mathbb{Z}_p$, denoted

x_i, $1 \le i \le n$.

D gives value x_i to P_i. x_i are public.

2) D computes $y_i = a(x_i)$ where

$a(x) = a_0 + \sum_{j=1}^{t-1} a_j x^j \bmod p$, where a_0 is the secret.

3) D gives the share y_i to P_i.

This is Shamir's SSS, does NOT work for

Here we need $\sum_{P_i \in A} y_i \ge T \iff A \in \Gamma$ and

$\sum_{P_i \notin A} y_i < T \iff A \notin \Gamma$.

The information rate is $\rho = \frac{1}{n}$

(t: threshold, n: number of players).

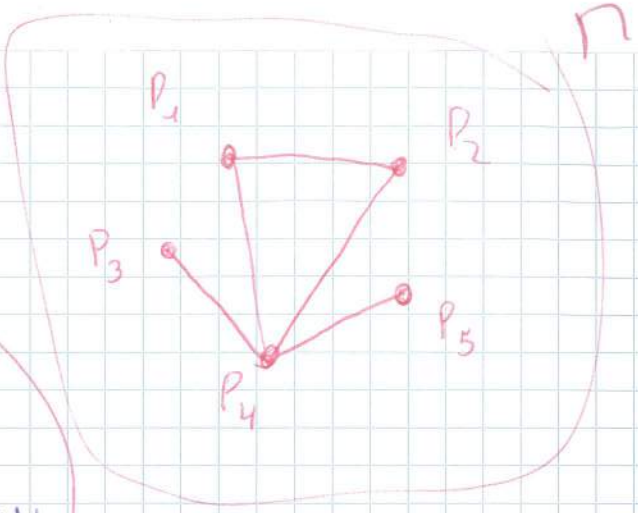
(4) c) SSS:

$\psi(D) = (1,1,1,1)$

Player	Shares
P_1	$\{(1,0,0,0),(0,0,1,0)\}$
P_2	$\{(1,0,0,0),(0,0,1,0)\}$
P_4	$\{(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$
P_3 *	$\{(0,0,0,1)\}$
P_5	$\{(0,0,0,1)\}$

WRONG

Information rate: $\rho = \frac{|S|}{\max_{P_i} |S_i|} = \frac{1}{3}$.



according to these vectors,

$\{P_1, P_2\} \notin \Gamma$

$\{P_4, P_5\} \notin \Gamma$ ...

(4) ~~a)~~ b) It must hold:

(1) $w_1 + w_2 \geq \overline{T}$

(2) $w_1 + w_4 \geq \overline{T}$

(3) $w_2 + w_3 \geq \overline{T}$

(4) $w_3 + w_4 \geq \overline{T}$

(5) $w_1 + w_3 < \overline{T}$

(6) $w_2 + w_4 < \overline{T}$

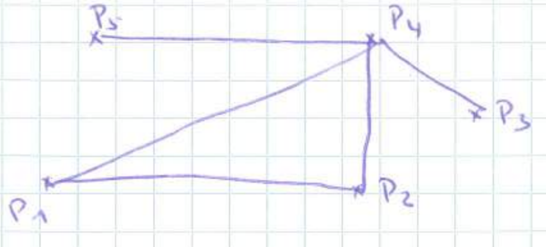
~~b)~~ (5) + 6) = $w_1 + w_3 + w_2 + w_4 < 2\overline{T}$, but

(1) + (4) = $w_1 + w_2 + w_3 + w_4 \geq 2\overline{T}$ ↯.

✓

c)

Γ_0:



→ Give P_3' and P_5 the same shares.

$\Gamma_0 = \{(P_1,P_2), (P_1,P_4), (P_2,P_4), (P_3,P_4), (P_4,P_5)\}$
$\quad B_1 \quad B_2 \quad B_3 \quad B_4 \quad B_5$

~~$\psi(D) = (1,1,1,1,1)$~~

~~Player~~	~~shares~~
~~P_1~~	~~$\{(1,0,0,0,0),(0,1,0,0,0)\}$~~
~~P_2~~	~~$\{(1,0,0,0,0),(0,0,1,0,0)\}$~~
~~P_3~~	~~$\{(0,0,0,1,0)\}$~~
~~P_4~~	~~$\{(0,1,0,0,0),(0,0,1,0,0),(0,0,0,1,0),(0,0,0,0,1)\}$~~
~~P_5~~	~~$\{(0,0,0,0,1)\}$.~~

~~Information rate $\rho = \frac{|S|}{\max_{P_i} |S_i|} = \frac{1}{4}$~~

~~If we give weight $w_i = |S_i|$ to every player with $T = 4$, we get a correct weighted threshold.~~

If we give weights as following:

P_1: $w_1 = 2$

P_2: $w_2 = 2$

P_3: $w_3 = 1$

P_4: $w_4 = 3$

P_5: $w_5 = 1$ and $T = 4$,

we get a correct weighted threshold.

(weights $= |S_i|$).

7/5//3 / 0 → 4.3

MAMME FME

Codes and Cryptography

Final Exam — 9 January 2015

Options: (Select one)

☐ **Only Coding** (only if you passed the Cryptography partial exam):
— Solve **all** the exercises in the Coding Theory part

☐ **Only Crypto** (only if you passed the Coding Theory partial exam):
— Solve **all** the exercises in the Cryptography part

☒ **Both parts**:
— Solve the items **marked with** *** in both parts

Coding Theory Part

*** 1. Consider the following family of binary codes $\mathcal{C}_{x,y} = \{0110, 01011, 101, xy\}$, for $x, y \in \{0, 1\}$. Determine which choices for x and y make the code uniquely decodable. Determine also which ones are prefix-free.

2. Given a non-uniform source with symbol probabilities

$$\mathcal{S} = (1/20, 5/20, 3/20, 2/20, 3/20, 4/20, 2/20)$$

build a binary Huffman code for it, and compute the corresponding average word length.

*** 3. Build a generating matrix of the 5-ary Hamming code of length 6. Give its dimension and minimum distance. Show also that it is perfect and MDS.

4. Build the generating matrix of a 7-ary cyclic code of length 8 and dimension 5. To that end, consider the following splitting into irreducible factors in $\mathbb{F}_7[X]$

$$X^8 - 1 = (X - 1)(X + 1)(X^2 + 1)(X^2 + 3X + 1)(X^2 - 3X + 1)$$

What can be deduced for this code from Singleton's bound?

By means of its dual code, build also a parity check matrix.

Cryptography Part

*** 1. Given a function family $\mathcal{F} = \{f_k : X_k \to Y_k\}_{k \in \mathcal{K}}$, define the following family of extended functions $\widehat{\mathcal{F}} = \{\widehat{f_k} : X_k \times X_k \to Y_k \times X_k\}_{k \in \mathcal{K}}$ such that $\widehat{f_k}(x, u) = (f_k(x), x \oplus u)$, where $\oplus$ denotes some (efficiently computable) group operation on X_k. Prove that $\mathcal{F}$ is one-way if and only $\widehat{\mathcal{F}}$ is one-way.

2. Catalano's public key encryption scheme is a variant of Paillier's that is more efficient but loses its homomorphic properties. The key generation is the same as in RSA, but the encryption function is $\text{Enc}(m) = r^e(1 + \tilde{m}n) \bmod n^2$, where $0 < r < n$ is a random integer and (n, e) is the public key.

   (a) Write in details the key generation procedure of RSA.

   (b) Design a decryption procedure, based on recovering the randomness r by means of the RSA decryption function.

   (c) Show that this encryption scheme does not have the homomorphic properties of Paillier's scheme.

*** 3. Consider the FDH-RSA signature scheme, with public key (N, e, H). Suppose a user P secretly obtains a valid signature σ on a public message m.

   (a) Give a 3-moves zero-knowledge proof of knowledge protocol where P proves knowledge of a valid FDH-RSA signature σ on public message m, for the public key (N, e, H), without revealing anything else on σ. Show the security properties of this zero-knowledge protocol. [**Hint:** σ is a pre-image of $H(m)$ for the homomorphic RSA permutation $f_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ defined by $f_e(x) = x^e \mod N$.]

   (b) Use the previous protocol to derive (via the Fiat-Shamir heuristic) an identity-based signature scheme, where the master entity knows the FDH-RSA secret key, and the secret key for a user with identity id is a FDH-RSA signature on the message $m = \text{id}$.

4. An access structure $\Gamma \subset 2^{\mathcal{P}}$ defined on a set of players $\mathcal{P} = \{P_1, \ldots, P_n\}$ is said to be *weighted threshold* if there exist positive integers $T, w_1, \ldots, w_n \in \mathbb{Z}^+$ such that, for any subset of players $A \subset \mathcal{P}$, we have $A \in \Gamma \Leftrightarrow \sum_{P_i \in A} w_i \geq T$.

   (a) Give a generalization of Shamir's threshold secret sharing scheme that works for a weighted threshold structure Γ. What is the information rate of the scheme ?

   (b) Prove that the access structure Γ defined by the basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}, \{P_1, P_4\}\}$, on a set of 4 players, is **not** weighted threshold.

   (c) Prove that the access structure Γ defined by the basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_4\}, \{P_2, P_4\}, \{P_3, P_4\}, \{P_4, P_5\}\}$, on a set of 5 players, is weighted threshold, and can be realized with a scheme with information rate $1/3$.

① Coding Theory Part

$C_{xy} = \{$ ~~00~~, 0110, 01011, 101, $xy\}$, $x, y \in \{0,1\}$

~~0110 101~~

✓ for 01 is not possible to be prefix free

✓ for 10 is not possible to be prefix free

Example ✓ 00 and 11 is possible.

with 01 ⇒ 0110 101 = 01 101 01 ✓

with 10 ⇒ 101 0110 = 10 101 10 ✓ } ↓ ✓ not uniquely decodable.

Sardinas - Patterson Theorem for ~~$\{00\} = \{xy$~~ $x=0, y=0$.

$C = \{0110, 01011, 101, 00\}$

$C_1 = \{0\}$ ~~$\{1\}$~~

$C_2 = \{110, 1011, 01, 0\} \Rightarrow C_1 \cap C_2$ ~~$\{01\}$~~

$C_3 = \{0\} = C_1$ ~~$\{00\}$~~

$\bigcup_{i=1}^{\infty} C_i = C_1 \cup C_2 = \{110, 1011, 01, 0\}$

(✓) Empty intersection with C , C is uniquely - decodable.

Sardinas - Patterson Theorem for $x=1, xy=1$.

$C = \{0110, 01011, 101, 11\}$

$C_1 = \{11\}$

$C_2 = \{01, 113\}$

$C_3 = \{1\} = C_1$

(✓) $\bigcup_{i=1}^{\infty} C_i = C_1 \cup C_2 = \{1, 01, 113\}$, empty intersection with C.

C is uniquely - decodable code

↳ C_{00} and C_{11} is prefix - free code, because 00 and 11 can not be a prefix of $\{0110, 10011, 101\}$

5b

③ Coding Part.

Build a G of 5-ary Hamming code of length 6.

- (1) Hamming codes are $[n, k, d]_q$ linear perfect codes with $d=3$ ✓
- (2) Singelton bound for a $[n, k, d]_q$ linear code is

$$k \leq n - d + 1$$

$$k \leq 6 - 3 + 1 = 4$$

↳ Build a Hamming code of $[6, 4, 3]_5$ in F_5^6

$q = 5$, ~~n=~~ $n = 6$, $k = 4$, min. distance $d = 3$

$$G = \left(\begin{array}{cccc|cc} 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 3 & 4 \\ 0 & 0 & 1 & 0 & 2 & 3 \\ 0 & 0 & 0 & 1 & 4 & 1 \end{array}\right) \quad \dim\ n \times k = 6 \times 4.$$

?!? How did you compute it?

$\begin{vmatrix} 2 & 3 \\ 4 & 1 \end{vmatrix} = 0$!!! (NOT MDS : $d = 2$)

- The dimension of the code is $4 = k$.
- The minimum distance is $d_c = \min_{x \in C, x \neq 0} d(x, 0) = \min_{x, y \in C, x \neq y} d(x, y)$

$d = 3$.

- sphere packing bound: $q^k = \dfrac{q^n}{(1 + n(q-1))}$ proof:

$$q^k = 5^4 = 625$$

$$\frac{q^n}{(1+n(q-1))} = \frac{5^6}{1 + 6(4)} = 625$$

↳ C is perfect, sphere packing bound is correct.

- Hamming code can correct only 1 error.
- MSD proove: $|C| \leq r^{n-d+1}$

$r^{n-d+1} = 5^{6-3+1} = 5^4 = 625$ ✓ ⇒ Hamming $[6, 4, 3]_5$ is MSD and perfect.

3 hojas

① Cryptography Part.

give: $\mathcal{F} = \{ f_k : X_k \to Y_k \}_{k \in K}$

$\hat{\mathcal{F}} = \{ \hat{f}_k : X_k \times X_k \to Y_k \times X_k \}_{k \in K}$

$\hat{f}_k(x,u) = (f_k(x), x \oplus u)$

prove $\mathcal{F}$ is OW if and only if $\hat{\mathcal{F}}$ is one-way.

If $\hat{\mathcal{F}}$ is not one-way, than we can compute from ~~$\hat{f}_k$~~ $f_k(x)$ a x and from $x \oplus u$ compute u.

Then $\mathcal{F}$ can be not one way, because $f_k(x) = y$ and we can compute with $\hat{\mathcal{F}}$ algoritm x from $\hat{f}_k(x,u)$.

→ Show an adversary and analyse the prob. distributions!

If $\tilde{\mathcal{F}}$ is one-way: (B - Algorithm for $\hat{\mathcal{F}}$)

(?) $\varepsilon_B = Pr[B(\hat{f}_k(x,u)) \in \hat{f}_k^{-1}(\hat{f}_k(x,u)), x \leftarrow X_k, u \leftarrow X_k]$ negl.

$\varepsilon_A = Pr[A(f_k(x,\blacksquare)) \in f_k^{-1}(f_k(x)), x \leftarrow X_k]$ must be negl.

③ Cryptography Part:

FDH - RSA signature scheme

① P chooses isomorphism ρ at random ~~de~~ and sends $K = \rho(x^e)$ to V.

② V chooses random bit $b \in \{0,1\}$ and sends b to P.

③ If $b=0$, P replies $f_e(x) = \rho$

If $b=1$, P replies $f_e(x) = \rho \circ f_e(x)$.

④ V outputs 1 iff $f_e(x) = x^e \bmod N$.

makes no sense at all, sorry.

10/10/9/8 → 9.3

MAMME FME

Codes and Cryptography

Final Exam — 9 January 2015

Options: (Select one)

☒ **Only Coding** (only if you passed the Cryptography partial exam):
— Solve **all** the exercises in the Coding Theory part

☐ **Only Crypto** (only if you passed the Coding Theory partial exam):
— Solve **all** the exercises in the Cryptography part

☐ **Both parts**:
— Solve the items **marked with** *** in both parts

Coding Theory Part

*** 1. Consider the following family of binary codes $\mathcal{C}_{x,y} = \{0110, 01011, 101, xy\}$, for $x, y \in \{0, 1\}$. Determine which choices for x and y make the code uniquely decodable. Determine also which ones are prefix-free.

2. Given a non-uniform source with symbol probabilities

$$\mathcal{S} = (1/20, 5/20, 3/20, 2/20, 3/20, 4/20, 2/20)$$

build a binary Huffman code for it, and compute the corresponding average word length.

*** 3. Build a generating matrix of the 5-ary Hamming code of length 6. Give its dimension and minimum distance. Show also that it is perfect and MDS.

4. Build the generating matrix of a 7-ary cyclic code of length 8 and dimension 5. To that end, consider the following splitting into irreducible factors in $\mathbb{F}_7[X]$

$$X^8 - 1 = (X - 1)(X + 1)(X^2 + 1)(X^2 + 3X + 1)(X^2 - 3X + 1)$$

What can be deduced for this code from Singleton's bound?

By means of its dual code, build also a parity check matrix.

Cryptography Part

*** 1. Given a function family $\mathcal{F} = \{f_k : X_k \to Y_k\}_{k \in \mathcal{K}}$, define the following family of extended functions $\widehat{\mathcal{F}} = \{\widehat{f}_k : X_k \times X_k \to Y_k \times X_k\}_{k \in \mathcal{K}}$ such that $\widehat{f}_k(x, u) = (f_k(x), x \oplus u)$, where $\oplus$ denotes some (efficiently computable) group operation on X_k. Prove that $\mathcal{F}$ is one-way if and only $\widehat{\mathcal{F}}$ is one-way.

2. Catalano's public key encryption scheme is a variant of Paillier's that is more efficient but loses its homomorphic properties. The key generation is the same as in RSA, but the encryption function is $\text{Enc}(m) = r^e(1 + mn) \bmod n^2$, where $0 < r < n$ is a random integer and (n, e) is the public key.

   (a) Write in details the key generation procedure of RSA.

   (b) Design a decryption procedure, based on recovering the randomness r by means of the RSA decryption function.

   (c) Show that this encryption scheme does not have the homomorphic properties of Paillier's scheme.

*** 3. Consider the FDH-RSA signature scheme, with public key (N, e, H). Suppose a user P secretly obtains a valid signature σ on a public message m.

   (a) Give a 3-moves zero-knowledge proof of knowledge protocol where P proves knowledge of a valid FDH-RSA signature σ on public message m, for the public key (N, e, H), without revealing anything else on σ. Show the security properties of this zero-knowledge protocol. [**Hint:** σ is a pre-image of $H(m)$ for the homomorphic RSA permutation $f_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ defined by $f_e(x) = x^e \mod N$.]

   (b) Use the previous protocol to derive (via the Fiat-Shamir heuristic) an identity-based signature scheme, where the master entity knows the FDH-RSA secret key, and the secret key for a user with identity id is a FDH-RSA signature on the message $m = \text{id}$.

4. An access structure $\Gamma \subset 2^{\mathcal{P}}$ defined on a set of players $\mathcal{P} = \{P_1, \ldots, P_n\}$ is said to be *weighted threshold* if there exist positive integers $T, w_1, \ldots, w_n \in \mathbb{Z}^+$ such that, for any subset of players $A \subset \mathcal{P}$, we have $A \in \Gamma \Leftrightarrow \sum_{P_i \in A} w_i \geq T$.

   (a) Give a generalization of Shamir's threshold secret sharing scheme that works for a weighted threshold structure Γ. What is the information rate of the scheme ?

   (b) Prove that the access structure Γ defined by the basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}, \{P_1, P_4\}\}$, on a set of 4 players, is **not** weighted threshold.

   (c) Prove that the access structure Γ defined by the basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_4\}, \{P_2, P_4\}, \{P_3, P_4\}, \{P_4, P_5\}\}$, on a set of 5 players, is weighted threshold, and can be realized with a scheme with information rate $1/3$.

(5.) We have the options $x_y = 00$
$x_y = 01$
$x_y = 10$
$x_y = 11$

By Sardinas-Patterson theorem A code C is uniquely decodable if and only if $C \cap (\bigcup_{k=1}^{\infty} C_k) = \emptyset$

$C_{x_y} = \{0110, 010111, 101, x_y\}$

C_2: If $x_y = 00$ $C_1 = \emptyset$ ✓

- $x_y = 01$ $C_1 = \{10, 0111\}$ ✓
  $C_2 = \{11, 01\}$ ✓
  $C_3 = \{\text{nonsense}\} \{01, 11\}$ ✓
  As $C \cap \bigcup_{k=1} C_k = \emptyset$ not valid

$C \cap C_3 = \{01\}$
For instance 0110101 can be decoded in two ways: 0110101 / 0110101 ✓

- $x_y = 10$ $C_1 = \{11\}$ ✓
  $C_2 = \{01, 01\}$, $01\}$ ✓
  $C_3 = \{10, 110, 1011\}$ ✓
  $, 011\}$,

✓ Again $C \cap C_3 \neq \emptyset$ so not valid
In this case 10101110 can be decoded: $10|10|110$ / $10|10|110$ ✓

- $x_y = 11$ $C_1 = \emptyset$

✓ So the options are $x_y = 00$ or $x_y = 11$ are in both cases we get a prefix-free code since $C_1 = \emptyset$. ✓

1

(10)

(2.) $S = (1/20, 5/20, 3/20, 2/20, 3/20, 4/20, 2/20)$ (0,05 0,25 0,15 0,1 0,15 0,2 0,1)

Huffman code:

First of all we orders them:

(0,25 0,2 0,15 0,15 0,1 0,1 0,05)

and compute $m = r - (-n+1) \bmod (r-1) = 2$

1) (0,25 0,2 0,15 0,15 0,1 0,1 0,05) — 0,1 0,05 → 0,15

2) (0,25 0,2 0,15 0,15 0,15 0,14) — 0,15 0,1 → 0,25

3) (0,25 0,25 0,2 0,15 0,15) — 0,15 0,15 → 0,3

4) (0,3 0,25 0,25 0,2) — 0,25 0,2 → 0,45

5) (0,45 0,3 0,25) — 0,3 0,25 → 0,55

6) (0,55 0,45)

16) (0) (1)

5) (1) (00) (01)

14) (00) (01) (10) (11)

13) (01) (10) (11) (000) (001)

12) (01) (11) (000) (001) (100) (101)

11) (01) (11) (000) (001) (101) (1000) (1001)

So the Huffman code is

$C = \{01, 11, 000, 001, 101, 1000, 1001\}$ ✓

The average word lenght: $L(C,S) = \sum_{i=1}^{n} l(w_i)\, p_i$

$L(C,S) = 2 \cdot 0,25 + 2 \cdot 0,2 + 3 \cdot 0,15 + 3 \cdot 0,15 + 3 \cdot 0,1$
$+ 4 \cdot 0,1 + 4 \cdot 0,05 = 2,7$ // ✓

(3) 5-ary Hamming code of length 6.

Hamming codes are $[n, k, d]_q$ - linear codes with $d = 3$.

$[6, k, 3]_5$

We can compute the parity check matrix:

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$ (6)

We defined H using 6 different directions

Now we compute G such that $GH^T = 0$ (5×6, 6×5)

$G =$

(9)

(3.) we can compute the parity check matrix, first of all we find m since $n = \frac{q^m-1}{q-1}$

$6 = \frac{5^m-1}{5-1} \Rightarrow 24 = 5^m - 1 \Rightarrow 5^m = 25 \Rightarrow \underline{\underline{m=2}}$

So we have 6 different directions:

$H = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$ (2, 1, 3) $\begin{pmatrix} 1 & 1 \\ 3 & 4 \end{pmatrix}$!!! ✓

the set distinct !!!

and $G = \begin{pmatrix} 0 & 3 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 0 & 1 & 1 \\ 4 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ $\begin{matrix} v \\ (v) \\ (v) \\ (v) \end{matrix}$ $\left(\begin{array}{cccccc} 0 & 3 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 0 & 1 & 1 \\ 4 & 1 & 0 & 1 & 1 & 1 \end{array}\right)$

(?!)

We know the dimension of the code corresponds to $k = n - m$, in our case $k = 6 - 2 = 4$ ✓

It is perfect since it meets the sphere packing bound: $q^k = \frac{q^n}{(1+n(q-1)} = \sum_{i=1}^{t} \binom{n}{i} (r-1)^i$

$5^4 = \frac{5^6}{(1+6(5-1))} \rightarrow 5^4 = \frac{5^6}{25} \Rightarrow 5^4 = 5^4$ ✓

Moreover it an MDS code since

$n - k + 1 = 6 - 4 + 1 = 3 = d$ ✓ (✓)

↳ you forgot to mention that $d = 3$ because it is a Hamming code! (and also because every 2 cols of H are l.i.)

(4.) 7-ary cyclic code of length 8 and dimension 5.

In order to do that we need a generater polynomial g such that $x^n - 1 \mid g$.

Moreover as $n = 8$ we must find a factor of degree $n - k = 8 - 5 = 3$. ✓

For instance choosing $g = (x+1)(x^2 + \cdots) =$

$= x^3 + x + x^2 + 1 = x^3 + x^2 + x + 1$ we have the generating matrix:

$$G = \begin{matrix} 1 & 1 \\ [8, 5]_7 \end{matrix}$$

For instance choosing $g = (x+1)(x^2 - 3x + 1) =$

$= x^3 - 3x^2 - x + x^2 - 3x - 1 = x^3 - 2x^2 - 4x - 1$

$$G = \begin{pmatrix} 1 & 5 & 3 & 6 & 0 & 0 & 0 & 0 \\ 0 & 1 & 5 & 3 & 6 & 0 & 0 & 0 \\ 0 & 0 & 1 & 5 & 3 & 6 & 0 & 0 \\ 0 & 0 & 0 & 1 & 5 & 3 & 6 & 0 \\ 0 & 0 & 0 & 0 & 1 & 5 & 3 & 6 \end{pmatrix} \quad (\checkmark)$$

We can decode from the singleton bound: $|\mathcal{C}| \leq r^{n-d+1} \Rightarrow r^k \leq r^{n-d+1}$

$7^5 \leq 7^{8-d+1} \Rightarrow 5 \leq 8 - d + 1 \Rightarrow d \leq 8 - 5 + 1 = 4$

$(n - k + 1)$

The dual code of C is generated by:

$$h(x) = (x-1)(x^2+1)(x^2+3x+1) = (x^3+x-x^2-1)(x^2+3x+1) =$$

$$= x^5+3x^4+x^3+x^3+3x^2+x-x^4-3x^3-x^2-x^2-3x-1 =$$

$$= x^5+2x^4-x^3+x^2-2x-1 \quad \checkmark$$

$$g^\perp(x) = x^5 h(x^{-1}) = x^5(x^{-5}+2x^{-4}-x^{-3}+x^{-2}-2x^{-1}-1) =$$

$$= -x^5-2x^4+x^3-x^2+2x+1 \quad \checkmark$$

and so

$$G^\perp = \begin{pmatrix} 6 & 5 & 1 & 6 & 2 & 1 & 0 & 0 \\ 0 & 6 & 5 & 1 & 6 & 2 & 1 & 0 \\ 0 & 0 & 6 & 5 & 1 & 6 & 2 & 1 \end{pmatrix} \quad \checkmark$$